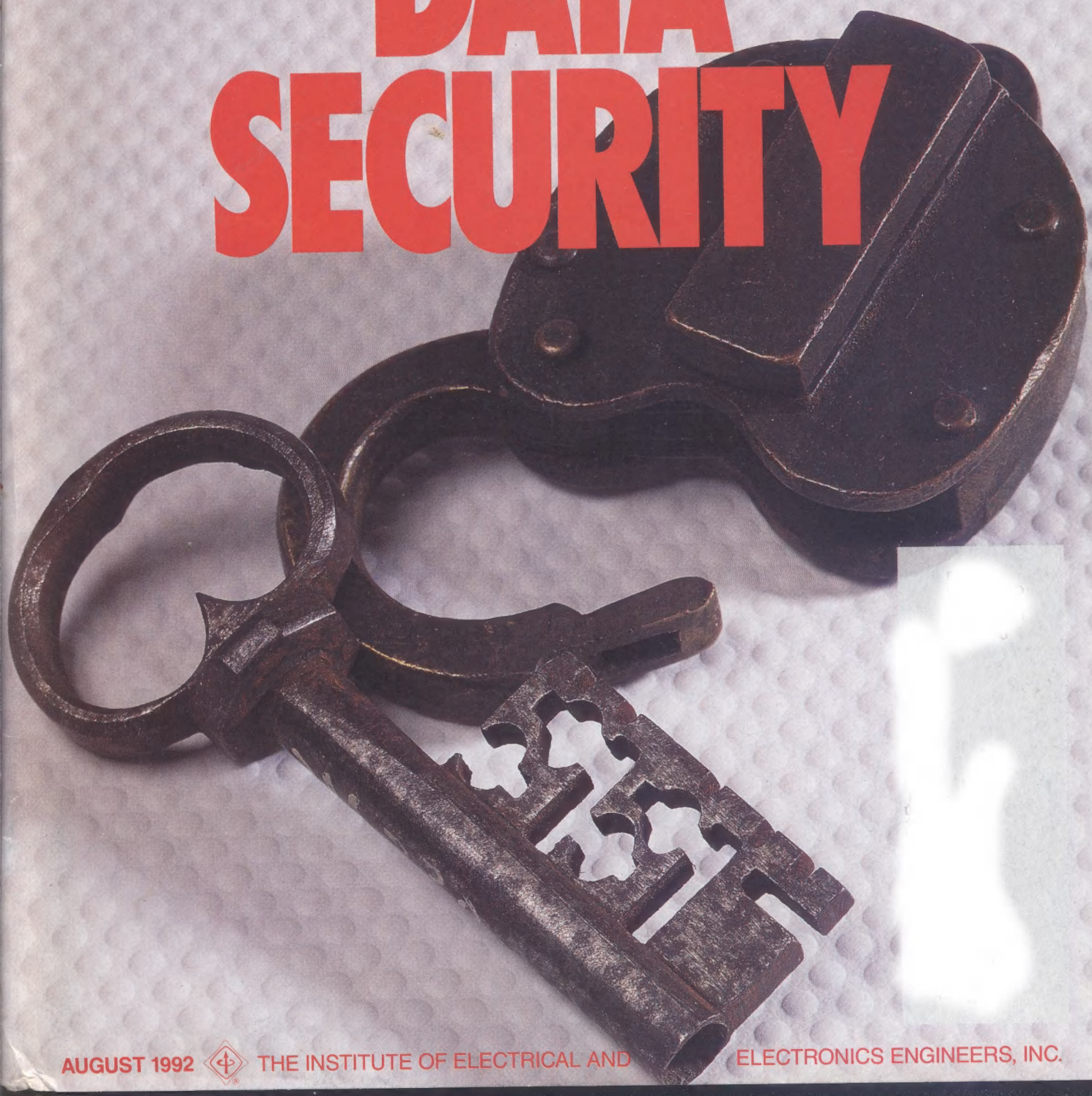
SUPERCONDUCTIVITY P. 50

IEEE

SPECTRUM

DATA SECURITY



AUGUST 1992 THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

IMAGE & SIGNAL PROCESSING, INC.

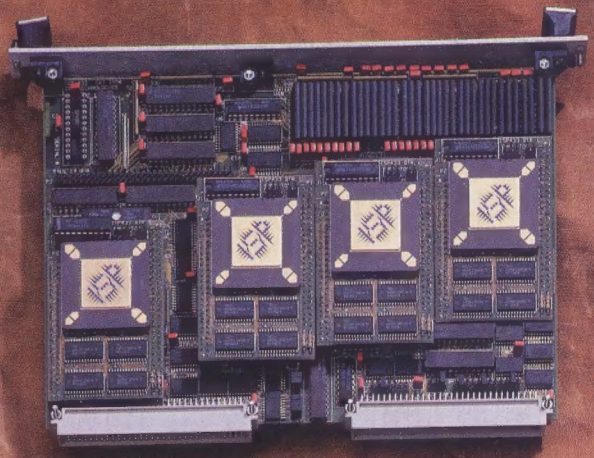
THE ARRAY OF POWER

Image & Signal Processing, Inc. designs and produces a large family of intelligent and "friendly" digital signal processing peripherals intended for use in high performance systems.

From complex FFT array processors to simple A/D converter boards, ISP® delivers an impressive selection of hardware and software products to satisfy the chaging needs of the engineering world.

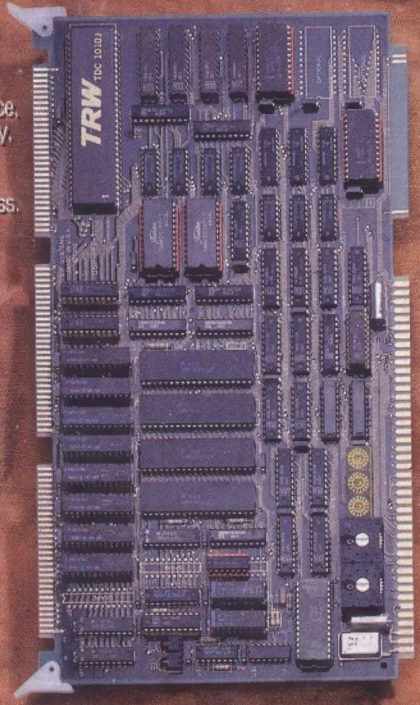
ISP's® veteran customer support team understands the intricacies involved with solving complicated and highly technical problems in an environment of tight budgets and impossible time constraints.

That's why high-technology companies from around the world now use the products designed and manufactured by ISP®.



ISP's® newest board, the RANGER™ is designed for imaging and data compression applications with high real-time data handling requirements. With one to four TMS320C30 floating point digital signal processors, the RANGER™ provides up to 133 MFLOPs and from 4 to 16 MBytes of fast DRAM. It also provides zero overhead data transfers between processing nodes, as well as VME and VSB master and slave capability. All processors are interlinked in addition to sharing the bus. Diagnostics, Utilities Math Libraries , and DSP/Signal Processing Algorithms are provided with the RANGER™. SPOX™ application libraries are also available.

ISP® produces Multibus® compatible single board mini-array processors, performing the sophisticated signal processing required for digital filters, complex FFT's, correlation, and convolution. ISP's® AP-6 can perform a 1024-point FFT in 8.5 msec. For a 1000-tap FIR digital filter, the bandwidth is 20 KHz. ISP's® Multibus® products provide performance, functionality, reliability, and cost effectiveness.



ISP's® POINT™ converts a PC into a powerful, cost-effective work station. Easy to use and versatile, the POINT™ is intended for a wide range of applications. ISP® offers several software products designed for the POINT™ series of MFLOP array processors, operational software and development software tools.

IMAGE & SIGNAL PROCESSING, INC.
120 Linden Avenue
Long Beach, CA 90802
Tel. 213 495-9533
Fax. 213 495-1258

CALL TODAY FOR A COMPLETE CATALOG: 213-495-9533

Circle No. 19

OMEGA Delivers...Fast!

Everything You Need for Process Measurement and Control

NEW!

Modular Vertical Recorders, 1-6 Channels

- Yt or X-Y Operation
- See F-41, P-9, Vol. 28 OMEGA Data Acquisition Handbook

600A Series
From **$2755 Complete**
Circle Reader Service Number 1
or Dial OMEGAfax and enter code: 1058

NEW!

Sensors Sold Separately

Flatbed Pen Recorders, 1-4 Channels

- Accepts dc Voltage, T/C and RTD Inputs
- See Page E-57, Vol. 28 OMEGA Data Acquisition Handbook

RD3720 Series
From **$1560**
Circle Reader Service Number 4
or Dial OMEGAfax and enter code: 1065

Multifunctional Digital Multimeter/Thermometer

- Measures, T/C's, RTD's, Voltage and Resistance
- See Page E-47, Vol. 28 OMEGA Data Acquisition Handbook

Model OM-7563
$1995
Circle Reader Service Number 2
or Dial OMEGAfax and enter code: 1064

NEW!

Sensors Sold Separately

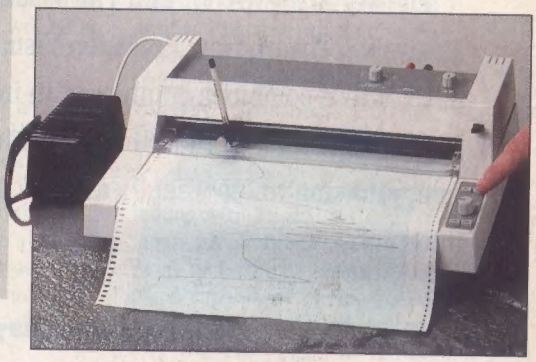
NEW!

Sensor Sold Separately

Multi-Functional Digital Multimeters

- 5½ and 6½ Digit Models
- See Page E-39, Vol. 28 OMEGA Data Acquisition Handbook

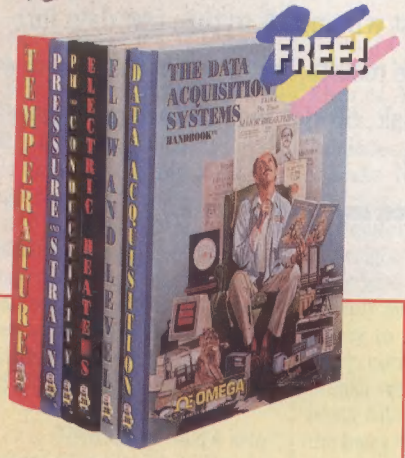
OM7550 Series
From **$895**
Circle Reader Service Number 3
or Dial OMEGAfax and enter code: 1342



Millivolt Single Pen Recorder

- Universal Pen Holder Accepts Any Pen up to 0.8 cm Diameter
- See Page F-62, Vol. 28 OMEGA Data Acquisition Handbook

Model RD545
$1150
Circle Reader Service Number 6
or Dial OMEGAfax and enter code:1239



FREE!

NEW, FREE Handbooks!
Over 4,000 Full-Color Pages

- More than 40,000 Items In Stock For Fast, Off-the-Shelf Delivery
- All Prices Listed
- Full of Technical Information

Circle Reader Service Number 5
or Dial OMEGAfax and enter code: 9989

IN A RUSH FOR HANDBOOKS?
DIAL

(203) 359-7874™
(203) 359-RUSH

OMEGAfax™

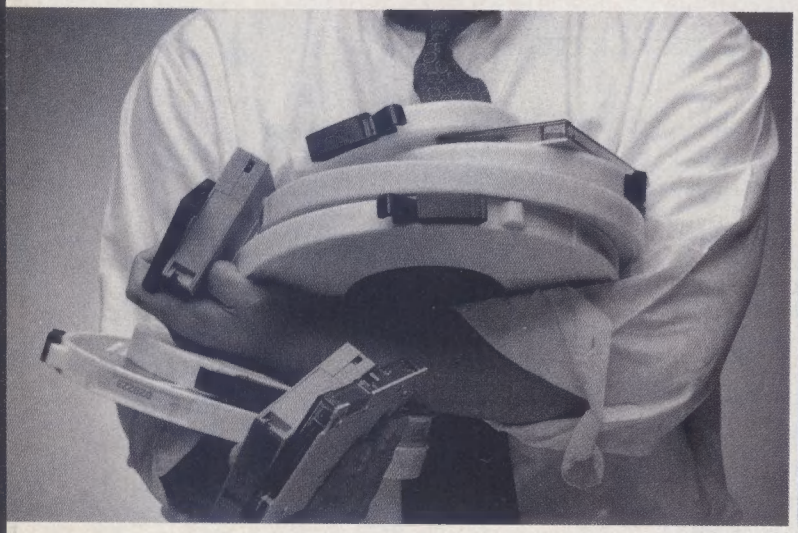
OMEGA's 24-Hour-a-Day, On-Demand Publishing System

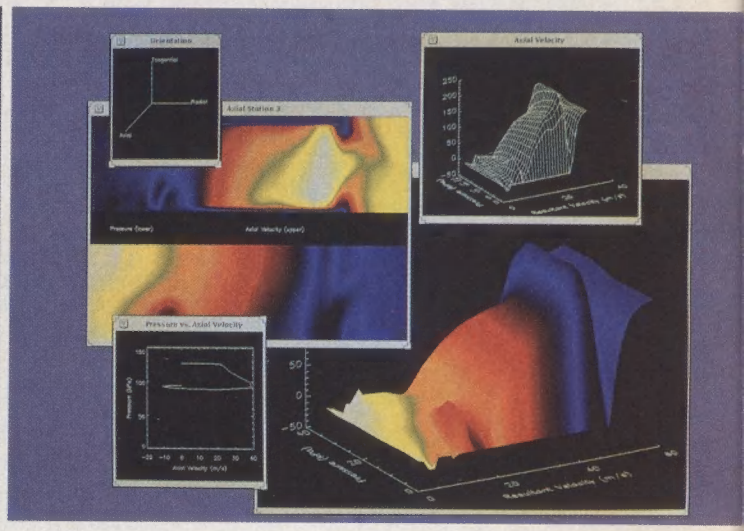
Call **1-800-848-4271**
from any Touch-Tone phone, and just enter the *OMEGAfax* numbers for the products you're interested in. A product specification sheet will be faxed to you automatically.
Don't forget to have your fax number handy!

OMEGA®
An OMEGA Technologies Company

One Omega Drive, Box 4047, Stamford, CT 06907
Telex 996404 Cable OMEGA FAX (203) 359-7700

RAW. WELL DONE.



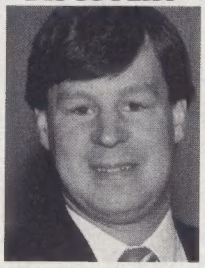


Attempting to analyze stacks of raw data can be frustrating if they can't be transformed into meaningful information that you can easily understand and use. Trends, relationships, insights, even breakthroughs, can remain buried unless you can unlock your data.

The key is PV-WAVE™ and The Visual Data Analysis Software from Precision Visuals.

PV-WAVE combines graphics with image processing, surface rendering, and animation, allowing you to visually analyze and interpret your data.

PV-WAVE™ TRANSFORMS DATA INTO DISCOVERY



"PV-WAVE gives me the power and flexibility of FORTRAN with the ease of use of my spreadsheet and a wide array of graphics capabilities."
Bill Estell
Analytical Engineer
United Technologies Hamilton Standard

With PV-WAVE, you can actually see your data, navigate through it, and display meaningful results. And, depending on your application, choose from point and click or command language versions for your Sun, DEC, HP, IBM, and SGI workstations and multi-user systems running UNIX, ULTRIX, and VMS.

If you're a scientist, engineer, researcher, or analyst who needs to turn raw data into well done results, call us today and ask about our no-risk, 60-day money-back guarantee!

Call Chris Logan today for your free video demo or evaluation copy of PV-WAVE.

1•800•447•7147

PV•WAVE™

The Visual Data Analysis Software

Precision Visuals, Inc. 6230 Lookout Road Boulder, Colorado 80301 USA (303) 530-9000

Circle No. 20

Newslog

JUNE 9. A consortium led by **ABB Asea Brown Boveri Ltd.**, Zurich, announced it had won a US $1.8 billion order to build an oil- and gas-fired power station and the world's biggest water desalination plant—producing 300 000 cubic meters of drinking water a year—in Abu Dhabi, United Arab Emirates. The power plant will have six 125-MW steam turbine units.

JUNE 11. Researchers at **Uniax Corp.**, Santa Barbara, Calif., said they had developed a device made of light-emitting polymers that can inexpensively replace semiconductor light sources in electronic objects, ranging from clocks to computers. The polymers can give off red, green, and other colors, and they are in liquid form, which can be coated on curved and angular surfaces to display information.

JUNE 11. **L. M. Ericsson** in Stockholm, the Swedish telecommunications company, said it had signed a purchasing agreement worth US $300 million for the supply of AXE digital telephone switching equipment to China. The order will extend the telecommunications network in Guangdong province.

JUNE 15. **ICL PLC** in London, the computer manufacturer in which Fujitsu Ltd. of Japan has a majority stake, and **Hughes STX Corp.**, headquartered in Lanham, Md., a subsidiary of Hughes Aircraft Co., said they would join forces to offer large customers security products to protect their computer networks against unauthorized intruders. The partnership will target international businesses that manage over 10 000 computer terminals.

JUNE 16. **IBM Corp.** said it is for the first time actively selling its own microchips to outsiders. The strategy marks a turnaround from IBM's traditional view that the output from its chip patents and factories was only to be consumed internally.

JUNE 17. A Federal district court jury in San Jose, Calif., ruled that **Advanced Micro Devices (AMD) Inc.**, Sunnyvale, Calif., in its clone of the 287 microprocessor produced by **Intel Corp.**, Santa Clara, Calif., does not have rights to use the microcode in Intel's chip. The decision may force AMD to start creating its own microcode.

JUNE 17. **The U.S. House of Representatives** voted to end the Federal financing of the US $8.3 billion Superconducting Super Collider particle accelerator, now being built in Texas. Over 18 000 contracts related to work on the collider have been let to thousands of companies and over 100 universities in 46 states. Supporters of the project said they hoped the Senate would restore the funding.

JUNE 19. **Northern Telecom Ltd.**, Mississauga, Ont., Canada, said it had developed a transmitting device whose light source needs to be aligned with an optical-fiber cable within 10–20 μm, compared with the current alignment of within 0.1 μm. Northern Telecom said its device is far cheaper to manufacture than current devices.

JUNE 22. A Federal appeals court in New York City ruled in favor of **Altai Inc.**, Arlington, Texas, against **Computer Associates International Inc.**, Islandia, N.Y., that Altai's use of a portion of a program for which Computer Associates holds the copyright did not violate that copyright. The decision may sharply limit large companies' ability to use copyrights to restrict competition. The ruling breaks with a 1987 Federal appeals ruling that has served as the basis for many highly visible cases argued over software protection in the last five years.

JUNE 22. **Groupe Bull** of France, **Olivetti** of Italy, and **Siemens-Nixdorf** of Germany said they had formed a joint venture, Trans European Information Systems, to develop trans-european systems for local public authorities. The aim is to make information technology services more available within the framework of the single European market.

JUNE 23. **Apple Computer Inc.**, Cupertino, Calif., and **Toshiba Corp.**, Tokyo, said they plan to jointly develop a multimedia product, blending text, graphics, video, and sound, for multiple markets, including entertainment, education, and information retrieval. The control software will be licensed from Kaleida, a joint venture of Apple and **IBM Corp.**

JUNE 27. **Japan's Ministry of International Trade and Industry (MITI)**, Tokyo, said it will sponsor the Real World Computing Project, a 10-year government-industry program to develop massively parallel computers, neural networks, and optoelectronics. Unlike the Fifth-Generation Computer Project that MITI closed down in June, the new effort will be an international one.

JUNE 29. Researchers at **AT&T Bell Laboratories**, Holmdel, N.J., said that, using extremely fast pulses of light, they had succeeded in transmitting 6.8 gigabits of information a second over a 840-km optical-fiber cable. Current lasers can send about 1.7 Gb/s.

JULY 4. **Casio Computer Co.**, Tokyo, said it had developed a foldable liquid-crystal display (LCD) about one-quarter the thickness of conventional products and weighing one-tenth as much. Casio said the LCD can easily be cut into different shapes, giving consumer electronics designers wider choices in conceiving new products.

JULY 8. A **Federal grand jury in New York City** said it had indicted five New York computer hackers, aged 18 to 22 years old, on charges of breaking into some of the most sensitive computers used by telephone companies and major credit card reporting services, and disrupting or stealing their data during a two-year period. The men face up to five years in prison for each of 11 counts [see related story, pp. 18–44].

JULY 9. The **National Aeronautics and Space Administration (NASA)** announced the landing of the **Space Shuttle Columbia** at Cape Canaveral, Fla., ending a two-week journey—the longest shuttle flight to date—for its crew of seven. While in flight, the crew grew protein crystals for medical research, studied fire safety in space, and jiggled drops of liquid with sound waves to see how fluids behave in space.

JULY 13. **Advanced Micro Devices Inc.**, Sunnyvale, Calif., and **Fujitsu Ltd.**, Tokyo, announced a US $700 million joint venture to develop, build, and market flash memories as well as erasable programmable read-only memory (EPROM) chips. The pact calls for each company to contribute $350 million to build a factory in Japan.

JULY 13. **IBM Corp.** said it is joining with **Toshiba Corp.** of Japan and **Siemens SA** of Germany to develop dynamic RAM chips capable of storing 256M bits of information. The joint effort will take place at IBM's semiconductor factory in East Fishkill, N.Y.

Preview:

AUG 28–SEP 5. The first **World Space Congress** is to be held in Washington, D.C., under the auspices of the National Academy of Sciences and NASA. The meeting will focus on space science, engineering, and policies for future space programs. For information, call 202-646-7569.

COORDINATOR: Sally Cahur

AUGUST 1992 Volume 29 Number 8

IEEE
SPECTRUM

PROFILE

62 Susan Hackwood

By TEKLA S. PERRY

As dean of a new engineering college at the University of California, Riverside, British-born electrical engineer Susan Hackwood is shaping a program that emphasizes the interdisciplinary fields of intelligent systems and environmental

Ron Mesaros

technologies. She is also demonstrating to aspiring female undergraduates that women engineers can successfully balance family and career.

BACK TO BASICS

65 The Smith chart

By JAMES E. BRITTAIN

When in the 1930s Phillip H. Smith, an engineer at Bell Telephone Laboratories, invented his soon-to-be-famous aid to transmission line analysis, analog methods of calculations abounded. Now, far from extinct, Smith's chart is alive and well in computer-based network analyzers and textbooks.

AWARDS

66 IEEE Field Awards

The 19 awards for 1992 went to 22 individuals for technical achievements in particular electrical and electronics engineering fields, including magnetic data storage, stochastic systems theory, and phased-array antennas.

Cover: Oh, for those bygone days when private papers and other important data could be made secure under lock and key, perhaps like these from the collection of the Smithsonian Institution/National Museum of American History. (Lock experts should note, however, that an unmatched combination was chosen for photographer Jim Pickerell for its photogenic value.) *Spectrum*'s Special Report on Data Security begins on p. 18.

IEEE SPECTRUM (ISSN 0018-9235) is published monthly by The Institute of Electrical and Electronics Engineers, Inc. All rights reserved. © 1992 by The Institute of Electrical and Electronics Engineers, Inc., 345 East 47th St., New York, N.Y. 10017, U.S.A. Cable address: ITRIPLEE. Telex 236-411. Fax: 212-705-7453. E-mail: ieeespectrum.

ANNUAL SUBSCRIPTIONS. IEEE members: $11.00 included in dues. Nonmembers: $29.95. Libraries/institutions: $139.

SINGLE COPIES. Members: $8 first copy, $16 per additional copy. Nonmembers: $16.

MICROFICHE SUBSCRIPTIONS. Members: $16. Nonmembers and libraries: $139.

POSTMASTER: Please send address changes to *IEEE Spectrum*, c/o Coding Department, IEEE Service Center, 445 Hoes Lane, Box 1331, Piscataway, N.J. 08855. Second Class postage paid at New York, N.Y., and additional mailing offices. Canadian GST #125634188.

Printed at 8649 Hacks Cross Rd., Olive Branch, Miss. 38654.

IEEE Spectrum is a member of the Audit Bureau of Circulations, the Magazine Publishers of America, and the Society of National Association Publications.

Forum

Saving the past

As companies combine or fail, and records are updated, much of our electro past is lost forever. While some organizations, such as the IEEE Center for the History of Electrical Engineering, are involved in chronicling the past, the average person can also help with documentation.

As company libraries "clean out the deadwood," some of us are in a position to retrieve items, sometimes by literally grabbing stuff from the dumpster. That's where I found a sheet metal panel with a schematic label that turned out to be the largest portion of a BC-785/SCR-270 radar transmitter found to date (the BC-785 is a later model than the BC-405/SCR-270 s/n 012 of Pearl Harbor fame, but used the same VT-122/WL-530 triode tubes, designed by Mouromtseff).

Do you have any books, manuals, instruction books, or catalogs lying about? Have you or any of your associates participated in projects or companies that could be recalled through interviews or documentation?

Contact: *RadarHist Newsletter*, Box 3087, Skokie, Ill. 60076-3087; 708-676-4629.

Donald A. Helgeson
Skokie, Ill.

Damage control

As chief scientist, Special Technologies Division, BMS Catastrophe, I would like to take issue with several of the technical statements in "Surviving hell and high water" [May, p. 44]. The author states that electronic equipment with chloride concentrations in excess of 1000 micrograms of chloride per square centimeter can successfully be restored. As reported by Barbara T. Reagor of Bellcore Labs, experience with the Hinsdale, Ill., switching office disaster has shown that concentrations in excess of 93 μg of sodium chloride equivalent per square centimeter has sustained irreversible damage (permeation of the noble metal surface) and cannot be reliably restored.

Much of the equipment from Hinsdale that was salvaged and "restored" by a third party firm has failed in service. Indeed, any concentration above 31 μg NaCl equivalent per square centimeter is cause for concern and special handling. As a professional restoration firm, we cannot recommend that electronic equipment with concentrations above the 93 μg NaCl equivalent per square centimeter level be "restored."

Another technical concern is the recommended "bake out" temperature in the cleaning protocol. The author has suggested 100° C for drying electronic assemblies. Our protocols call for a maximum of 60° C to prevent damage to the elastomers and other components of electronic assemblies such as cathode-ray tube monitors. Such excessive temperature can also cause problems with bearing lubricants on precision electromechanical components in floppy-disk drives and other storage media.

I must also protest our company's exclusion from the list in the article. BMS Catastrophe has headquarters at 303 Arthur St., Fort Worth, Texas 76107; 800-433-2940. The Canadian office (BMS Catastrophe Ltd.) is at 6535 Millcreek Dr., Unit 2 & 3, Mississauga, Ont. L5N2M2, Canada; 416-567-4400. The Australian office (BMS Castastrophe Australia) is at 23 Jarrah Dr., Victoria, Australia; (61+3) 587 69 45.

L. D. Dave McDaniel
Fort Worth, Texas

In support of diversity

I read "Diversity in the high-tech workplace" [June, p. 20] with fascination. I was pleased to see increasing recognition of diverse races and of women in the workplace, and above all of diverse sexual orientations. The article omitted listings of gay/bi/lesbian groups; I can add these:

- High-Tech Gays, Box 6777, San Jose, Calif. 95150-6777; voice mail, 408-993-3830; BBS 415-572-9594, 300-2400 BPS.
- Lesbian and Gay-Affiliated Engineers and Scientists (LGAES), Box 70 133, Sunnyvale, Calif. 94086-0133.
- National Organization of Gay and Lesbian Scientists and Technical Professionals (NOGLSTP), Box 91 803, Pasadena, Calif. 91109-9813.

It would be nice if diversity at work included dress; your cover, showing all the males wearing traditional business attire, is somewhat discouraging, and tales still abound of companies with stiff dress codes. Personally I would like to see ties and suits being optional for all occasions, and shorts being welcomed everywhere.

Roger A. C. Williams
Boulder, Colo.

As an African-American male engineer, I read with interest "Diversity and performance in R&D" and the associated articles. It was disheartening to see what little progress U.S. companies have made in integrating the engineering workforce.

The statement " . . . there is not more overt evidence of discrimination and exclusion for 'new' groups in R&D on the part

(Continued on p. 11)

Calendar

Meetings, Conferences and Conventions

AUGUST

Atomic and Nanoscale Modification of Materials: Fundamentals and Applications (ED); Aug. 16–21; Doubletree Hotel, Ventura, Calif.; Gordon Fisher, Cornell University, 423 Hollister Hall, Ithaca, N.Y. 14853; 607-255-7578.

International Symposium on Electromagnetic Compatibility (EMC); Aug. 18–20; Anaheim Marriott Hotel, Anaheim, Calif.; George M. Kunkel, Spira Manufacturing Corp., 12721 Saticoy St. South, North Hollywood, Calif. 91605; 818-764-8222.

Advanced Technology Workshop on Influence of Temperature on Microelectronic Device Failure Mechanisms (RS); Aug. 25; Center of Adult Education, University of Maryland, College Park; Pradeep Lall, Calce Electronics Packaging Research Center, University of Maryland, College Park, Md. 20742; 301-405-5323.

International Conference on Solid-State Devices and Materials (EDS); Aug. 26–28; Daiichi Hotel, Tsukuba, Japan; Mitsuo Kawabe, Institute of Materials Science, University of Tsukuba, Ibaraki 305, Japan; (81+298) 53 5066.

International Symposium on Applications of Ferroelectrics (UFFC); Aug. 31–Sept. 2; Hyatt Regency Greenville, Greenville, S.C.; Gene Haertling, 206 Olin Hall, Clemson University, Clemson, S.C. 29634-0907; 803-656-0180.

SEPTEMBER

Second Singapore International Conference on Image Processing—ICIP '92 (Region 10); Sept. 7–11; Marina Mandarin Singapore Hotel, Singapore; ICIP '92 Secretariat, IEEE Singapore Section, 200 Jalan Sultan, 11–03 Textile Centre, Singapore 0719; (65) 291 9690; fax, (65) 292 8596.

Symposium on High Performance Distributed Computing (C); Sept. 9–10; Sheraton Hotel, Syracuse, N.Y.; IEEE Computer Society, Conference Department, 1730 Massachusetts Ave., N.W., Washington, D.C. 20036-1903; 202-371-1013; fax, 202-728-0884.

Cement Industry Conference (IA); Sept. 11; Doubletree Hotel, Tucson, Ariz.; Fran Young, Arizona Portland Cement, Box 338, Rillito, Ariz. 85654; 714-683-3660.

Fifth Digital Signal Processing Workshop (SP); Sept. 13–16; Starved Rock Lodge, Starved Rock State Park, Ill.; Mark J.T. Smith, School of Electrical Engineering, Georgia Institute of Technology, Atlanta, Ga. 30322-0250; 404-894-6291.

International Conference on Control and Applications (CS, Dayton Section); Sept. 13–16; Stouffer Center Plaza Hotel, Dayton, Ohio; Daniel W. Repperger, Armstrong Laboratory, Wright Patterson AFB, Dayton, Ohio 45433-6573; 513-255-5742; fax, 513-255-9687.

Electrical Overstress/Electrostatic Discharge Symposium (CHMT); Sept. 15–18; Loew's Anatole Hotel, Dallas; EOS/ESD Association, 200 Liberty Plaza, Rome, N.Y. 13440; 315-339-6937; fax, 315-339-6793.

Conference on Wireless LAN Implementation (C); Sept. 17–18; Dayton Convention Center, Dayton, Ohio; IEEE Computer Society, Conference Department, 1730 Massachusetts Ave., N.W., Washington, D.C. 20036-1903; 202-371-1013; fax, 202-728-0884.

42nd Annual IEEE Broadcast Symposium (BT); Sept. 17–18; Hotel Washington, Washington, D.C.; Edmund A. Williams, Public Broadcasting Service, 1320 Braddock Place, Alexandria, Va. 22314; 703-739-5172; fax, 703-739-8938.

Virtual Reality Annual International Symposium (NN); Sept. 18–23; Sheraton Hotel, Seattle, Wash.; Thomas Caudell, Boeing Computer Services, Boeing Building 33-07, MS 7L-22, 2760 160th Ave. S.E., Bellevue, Wash. 98008; 206-865-3763.

Autotestcon '92 (AES, IM, Dayton Section); Sept. 21–24; Dayton Convention Center, Dayton, Ohio; Kenneth Wilkinson, Ateam Corp., 7920 Chambersburg Rd., Dayton, Ohio 45424; 513-237-7971; fax, 513-237-7974.

Application Specific Integrated Circuits Conference and Exhibit (C, Rochester Section); Sept. 21–25; Rochester Riverside Convention Center, Rochester, N.Y.; Lynne M. Engelbrecht, ASIC Seminar Coordinator, 170 Mount Read Blvd., Rochester, N.Y. 14611; 716-328-2310; fax, 716-436-9370.

13th International Semiconductor Laser Conference (LEO); Sept. 21–25; Takamatsu Kokusai Hotel, Takamatsu, Japan; 13th IEEE International Semiconductor Laser Conference, Business Center for Academic Societies Japan, 3-23-1, Hongo, Bunkyo-ku, Tokyo 113, Japan; (81+3) 3817 5831; fax, (81+3) 3817 5836.

International Test Conference (C, Philadelphia Section); Sept. 22–24; Baltimore Convention Center, Baltimore, Md.; Doris Thomas, International Test Conference, 514 E. Pleasant Valley Blvd., Suite 3, Altoona, Pa. 16602; 814-941-4666; fax, 814-941-4668.

Petroleum and Chemical Industry Technical Conference (IA); Sept. 28–30; River City Marriott Hotel, San Antonio, Texas; Knox Pitzer, Thermon Manufacturing Co., 100 Thermon Dr., Box 609, San Marcos, Texas 78666; 512-396-5801; fax, 512-396-3627.

13th International Electronics Manufacturing Technology Symposium (CHMT); Sept. 28–30; Hyatt Regency Inner Harbor Hotel, Baltimore, Md.; Bill Moody, 2529 Eaton Rd., Wilmington, Del. 19810; 302-478-4143; fax, 302-478-7057.

First IEEE International Conference on Universal Personal Communications (COM, Dallas Section); Sept. 29–Oct.1; Loews Anatole Hotel, Dallas; Dhawal Moghe, Bell Northern Research, 1150 E. Arapaho Rd., Richardson, Texas 75081; 214-997-4506; fax, 214-997-4792.

IEEE members attend more than 5000 IEEE professional meetings, conferences, and conventions held throughout the world each year. For more information on any meeting in this guide, write or call the listed meeting contact. Information is also available from: Conference Services Department, IEEE Service Center, 445 Hoes Lane, Box 1331, Piscataway, N.J. 08855; 908-562-3878; submit conferences for listing to: Ramona Foster, *IEEE Spectrum*, 345 E. 47th St., New York, N.Y. 10017; 212-705-7305.

For additional information on hotels, conference centers, and travel services, see the Reader Service Card.

ure diversity. Im-
outreach programs
ill maximize the op-
These programs can
e minds of children
nder of mathemat-
ng challenging en-
roblems at univer-
search. Success of
nds on a willingness
and work hand in

U.S. industry must
manager to imple-
ograms. This non-
serve to achieve a
archers, and elimi-
ceilings and walls
uctively.

Alfred R. Paiz
Pasadena, Calif.

count

ster, the engineer-
prouted yet anoth-
nale shortage myth.
p. 21] that native-
stitute only 15 per-
in the number of
d 2000 is very mis-
his statistic means
is, the numerical
tforce entrants and
native-born white
15 percent of the
as a whole. How-
nificant here is the
of all workforce en-
white males are ex-
s 32 percent of this

wrence Fafarman
os Angeles, Calif.

den

Radio Propagation
nications Research
nent of Canada's
unications, I was
eddes' letter con-
Fessenden's con-
nunications [June,
ting, however, is to
ddes' letter.
o telegraphy trans-
tic Ocean [in spring
gh-frequency (HF)
able HF alternator
re the fall of 1906.
ered by the Gener-
capable of running
nerate frequencies
Machrihanish and

(Continued on p. 70)

Cale

Meetings, Conferer

AUGUST

Atomic and Nanoscale Modification of Materials: Fundamentals and Applications (ED); Aug. 16–21; Doubletree Hotel, Ventura, Calif.; Gordon Fisher, Cornell University, 423 Hollister Hall, Ithaca, N.Y. 14853; 607-255-7578.

International Symposium on Electromagnetic Compatibility (EMC); Aug. 18–20; Anaheim Marriott Hotel, Anaheim, Calif.; George M. Kunkel, Spira Manufacturing Corp., 12721 Saticoy St. South, North Hollywood, Calif. 91605; 818-764-8222.

Advanced Technology Workshop on Influence of Temperature on Microelectronic Device Failure Mechanisms (RS); Aug. 25; Center of Adult Education, University of Maryland, College Park; Pradeep Lall, Calce Electronics Packaging Research Center, University of Maryland, College Park, Md. 20742; 301-405-5323.

International Conference on Solid-State Devices and Materials (EDS); Aug. 26–28; Daiichi Hotel, Tsukuba, Japan; Mitsuo Kawabe, Institute of Materials Science, University of Tsukuba, Ibaraki 305, Japan; (81+298) 53 5066.

International Symposium on Applications of Ferroelectrics (UFFC); Aug. 31–Sept. 2; Hyatt Regency Greenville, Greenville, S.C.; Gene Haertling, 206 Olin Hall, Clemson University, Clemson, S.C. 29634-0907; 803-656-0180.

SEPTEMBER

Second Singapore International Conference on Image Processing—ICIP '92 (Region 10); Sept. 7–11; Marin Mandarin Singapore Hotel, Sin gapore; ICIP '92 Secretariat IEEE Singapore Section, 20 Jalan Sultan, 11–03 Textil Centre, Singapore 0719; (65 291 9690; fax, (65) 292 8596.

Symposium on High Perfor mance Distributed Comput ing (C); Sept. 9–10; Sherato Hotel, Syracuse, N.Y.; IEE Computer Society, Conferenc Department, 1730 Mas sachusetts Ave., N.W., Washing ton, D.C. 20036-1903; 202-371 1013; fax, 202-728-0884.

Cement Industry Confer ence (IA); Sept. 11; Doubletre Hotel, Tucson, Ariz.; Fra Young, Arizona Portland Ce ment, Box 338, Rillito, Ariz 85654; 714-683-3660.

Fifth Digital Signal Process ing Workshop (SP); Sept. 13- 16; Starved Rock Lodge Starved Rock State Park, Ill. Mark J.T. Smith, School of Elec trical Engineering, Georgi Institute of Technology, Atlan ta, Ga. 30322-0250; 404-894 6291.

International Conferenc on Control and Application (CS, Dayton Section); Sept 13–16; Stouffer Center Plaz Hotel, Dayton, Ohio; Daniel W Repperger, Armstrong Labora tory, Wright Patterson AFB Dayton, Ohio 45433-6573; 513 255-5742; fax, 513-255-9687.

Electrical Overstress/Elec trostatic Discharge Sympo sium (CHMT); Sept. 15–18 Loew's Anatole Hotel, Dallas EOS/ESD Association, 200 Lib erty Plaza, Rome, N.Y. 13440 315-339-6937; fax, 315-339 6793.

Conference on Wireles LAN Implementation (C) Sept. 17–18; Dayton Convention Center, Dayton, Ohio; IEE Computer Society, Conference

Forum

(Continued from p. 6)

of either supervisors or colleagues'' was not supported by the facts stated earlier in the article. Perhaps the authors were looking for pure racist/sexist attacks, but given the method by which the researchers received their survey data (at meetings held on the company's premises and through the mail), frank (and honest) opinions would not be ascertained. It does a great disservice to both U.S. corporations and their employees by not placing racism/sexism in the workplace in a clear perspective.

In general, the companies showcased were exceptions to the typical engineering environment. There exists great disparity between the U.S.-born white males and other groups. In most companies, this is explained by statements such as ''we can't find qualified applicants'' and ''he/she doesn't have enough experience.'' Such rationalizations continue institutional bigotry.

Many U.S. corporations continue the ''old boy network'' to the detriment of the corporations' growth and the country's need for a well-trained workforce. I hope that this article may cause some executives to look again at their company's diversity and search in earnest for ways of expanding its workforce.

Ellis L. Glispie
Washington, D.C.

A key finding of the report on workforce diversity indicates that we must now minister to the foreign-born researchers who work in U.S. R&D. Certainly the conclusion is proper, but the troublesome missing data on U.S.-born ''nontraditionals'' and sparse data on U.S.-born women suggest that we are not yet seeing the positive effects of diversity. It seems to me that if the United States, nearly 50 years after World War II, is still struggling to bring U.S.-born minorities and women into the R&D workplace, achieving nondiscriminatory diversity becomes more difficult.

To work effectively within this potentially contradictory environment, I believe that we first-line R&D managers must implement proactive diversity programs within our immediate organizations. This activism will allow us to manage the difficult conjoint task of providing our U.S.- and foreign-born minorities and women with equal access to U.S. R&D. A critical aspect of this problem involves assuring all men and women entering the U.S. R&D workforce of a nurturing environment for obtaining the training and opportunities needed to achieve technical excellence and career promotion.

As with all socioeconomic problems, there are no magic solutions to multiculturalism. Building partnerships with the U.S. educational system represents a workable approach to achieving future diversity. Implementing educational outreach programs at all educational levels will maximize the opportunities for success. These programs can range from stimulating the minds of children with the beauty and wonder of mathematics and science to funding challenging engineering and scientific problems at universities not known for research. Success of these partnerships depends on a willingness to roll up shirtsleeves and work hand in hand.

For diversity to occur, U.S. industry must empower the first-line manager to implement bold, innovative programs. This nontraditional approach will serve to achieve a rainbow coalition of researchers, and eliminate the pervasive glass ceilings and walls that now serve us destructively.

Alfred R. Paiz
Pasadena, Calif.

Demanding a recount

That hydra-headed monster, the engineering shortage myth, has sprouted yet another head: the U.S. white-male shortage myth.

The statement [June, p. 21] that native-born white men will constitute only 15 percent of the ''increase'' in the number of workers between 1985 and 2000 is very misleading. Basically, what this statistic means is that the growth—that is, the numerical difference between workforce entrants and workforce leavers—of the native-born white male workforce will be 15 percent of the growth of the workforce as a whole. However, what is really significant here is the composition of the group of all workforce entrants, and non-Hispanic white males are expected to be an enormous 32 percent of this group.

Lawrence Fafarman
Los Angeles, Calif.

More on Fessenden

As the director of the Radio Propagation Laboratory in the Communications Research Centre in the Government of Canada's Department of Communications, I was pleased to read L. A. Geddes' letter concerning Reginald Aubrey Fessenden's contributions to radio communications [June, p. 6]. My purpose in writing, however, is to point out an error in Geddes' letter.

The first two-way radio telegraphy transmissions across the Atlantic Ocean [in spring 1906] did not employ high-frequency (HF) alternators, since a suitable HF alternator was not developed before the fall of 1906. The HF alternator delivered by the General Electric Co. was only capable of running at speeds that would generate frequencies up to about 10 kHz. The Machrihanish and

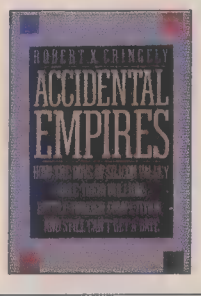
(Continued on p. 70)

Books

Poison pen potpourri

Larry Kaplan

Accidental Empires: How the Boys of Silicon Valley Make Their Millions, Battle Foreign Competition, and Still Can't Get a Date. *Cringely, Robert X., Addison-Wesley, New York, 1992, 324 pp., US $19.95.*



It's hard to like a book whose title, preface, and first chapter antagonize, ridicule, and deride the very industry and people who might benefit from reading it. The author lumps his readers into hate groups, belittles the entire computer industry, and portrays its leaders as childish egomaniacs.

Robert X. Cringely is the pen name of a weekly gossip columnist for *Infoworld*, an industry newspaper, and his gossipy tale of the personal computer industry is only the latest of many attempts to chronicle that business. Most, though, have been serious analyses, and Cringely's will never be consigned to that category.

The book begins by blaming the personal computer for the excesses of consumerism, the insider trading scandals, and the recessions. Cringely then lays out his premise: that the personal computer happened by accident, created by amateurs who remain amateurs. His targets include the usual suspects: William H. Gates, Steven Jobs, and IBM Corp.

Cringely lambasts Bill Gates for all manner of transgressions, including parsimony, hiring slave laborers, and dealing in "vaporware" (software that is hyped by a company but never released). One story has Gates, a multibillionaire, holding up a line of people to find a coupon for ice cream he is buying. One of the other patrons gives Gates fifty cents, which he accepts. Another tale has Gates refusing to hire any other people named Bill until Microsoft had 500 employees. Gates is also criticized for hiring fresh college graduates and burning them out. Microsoft is held to be the height of mediocrity.

Steve Jobs comes under fire for sociopathic behavior such as ruining careers and marriages. He is cast as a "willful kid who'd always resented the fact that he had been adopted." Apple is characterized as an anarchic, non-adult-supervised mess.

IBM, of course, is the most evil of companies. "IBM people are a little smug, a little slow, and slightly overweight," Cringely writes. In his view, the company has no soul, no creativity, and no discernible brain activity. All IBM employees want is more power, to move up the corporate ladder and have their cars washed "every Saturday, paying extra to get the hot wax." IBM lies to its customers, to its developers, and to its vendors, and destroys its competition by purveying vaporware and by creating its own standards.

Cringely uses infamous people for many comparisons. Jobs is painted like both Bhagwan Rajneesh and Jim Jones in one paragraph. Gates is portrayed as Kim Il Sung of North Korea. Jean-Louis Gassée's staff meetings become Stalinesque.

After blasting every one in sight, Cringely gives his description of how things ought to be. He likens a start-up company to an army waging war, with wave after wave of soldiers. The commandos—the first wave—are the founders, who make success possible by their creativity. The infantry, the second wave, make success happen with their ability to build an infrastructure that manufactures and sells the product. The third wave, the police, maintain and service old product lines. Peril lies in the troughs between waves.

Cringely says that for the United States to have a future in computing, it must forget about hardware and concentrate on software, using the movie studio as the basis for a proposed software studio. It must use an infrastructure like the movie industry, with a central financing, marketing, distribution, and administration catering to groups of entrepreneurs creating new products.

Although there are some fresh new insights and stories in the book, most are oft-repeated industry myths. Cringely's sources are primarily engineers who call his office (he gives the number 415-312-0555, if anyone's interested) or send him items by fax or electronic mail. Since these engineers tend to be the disgruntled ones, the information is usually negative and bitterly critical. Cringely ends up with a very biased view of the computer industry and its leaders.

The book's title is cute but misleading and clearly belongs on a different book. Very few foreign competition battles are detailed; there are no examples of anyone having trouble getting a date, and really almost no evidence that there are any empires, accidental or not. The "boys" did make millions, but mostly by design and hard work. A better title for the book would have been *Computer Tales: How I make money from gossip by meeting and trashing rich and famous people.*

In fact, one of the puzzling aspects of this book is the author's use of a pen name. The author drops enough names, quotes enough people, and meets with enough industry leaders for it to be hard to imagine they don't know who he is. Certainly, Mitch Kapor, who had to use Cringely's home bathroom, must know. Unless, of course, Cringely has all his mail, prescription bottles, and personal identification covered up or removed every day. Or worse, he has taken on the identity of Cringely permanently (a distinct possibility, since my review copy was actually signed "Bob Cringely").

Cringely's assertions that the personal computer created rampant consumerism, insider trading, and the recession are left hanging: nothing else in the book backs them up. The movie studio analogy is not new and is at best a mistake (although Tom Peters, the author, praised it in a recent column). Current movie studio infrastructures are doing worse than their full-service studio counterparts. Orion, Carolco, Cannon, and Tri-Star are all going under, precisely because they have nothing without the typical studio base of workers, creative and otherwise, who are loyal to each other.

The analysis of computer start-up as war, like many analogies in the book, paints black pictures of the computer industry. Many employees actually enjoy their lives and their jobs. And many "consort" with the "enemy." In fact, many start-ups are formed by individuals from competing companies who find a common bond. To endanger this element of the industry would be a mistake.

A start-up company can be a magical place. People are focused on something that is at first abstract and far in the future. Then they form a team, and interact with each other in unique and complex ways in order to create something concrete and not so far in the future.

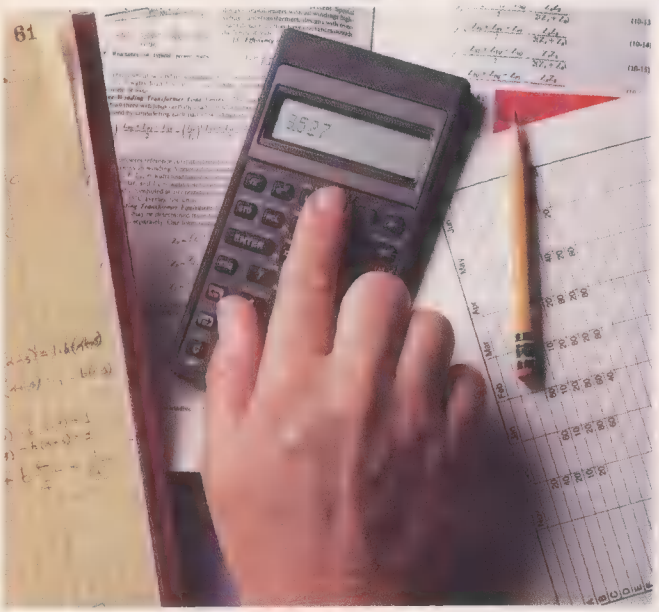
As in any human endeavor, there are moments of happiness, sadness, frustration, and exhilaration. Whether successful or not, the new company creates in its employees feelings that are difficult to achieve anywhere else. Probably as many careers and marriages are made as are ruined. It seems that Cringely and his sources have never felt or at least communicated these feelings. They have missed the magic that is at the heart of every Silicon Valley, wherever and whenever they happen to be.

Larry Kaplan used to design video games for a liv-

(Continued on p. 68)

There are two ways to do your math.

Drag.



Click-n-drag.

Solve problems fast with Mathcad 3.1.

Don't let calculations keep you from getting work done. Cruise through problems with the math package that's fast, all-purpose—and easy: Mathcad 3.1.

The one-step system.

Mathcad 3.1 is much more than just a number-cruncher. It's an integrated math *system* that performs everything from addition to symbolics—easily and naturally. Because it works the way you think.

Just type your calculations anywhere on the screen—just like a scratch pad—and you're done. Mathcad does the calculating. Updates answers when a variable changes. Graphs in 2-D or 3-D. Even accepts bitmapped graphics.

A quick menu pick gives you full symbolic calculation capabilities. So you can do any integral, Taylor series, or infinite sum with click-n-drag simplicity.

Done calculating? Mathcad prints out presentation-quality documents complete with equations in real math notation.

PC MAGAZINE THE BEST OF 1991 COVER STORY

Give your math a hand.

To help you work even faster, Mathcad 3.1 includes a Standard Electronic Handbook for instant access to hundreds of standard formulas, useful data, and commonly-used equations. Ready for interactive use, just click-n-paste them into your work. Without ever opening a reference book.

And now there are three new optional Electronic Handbooks,* created with the leading publishers of technical handbooks: The CRC Materials Science and Engineering Handbook, Machine Design and Analysis from McGraw-Hill, and the Mathcad Treasury of Methods and Formulas. Plus optional Applications Packs with modifiable templates for all major engineering and science fields.

PC MAGAZINE EDITOR'S CHOICE

Mathcad 2.5
3-14-89 issue.
Best of '88
Best of '87

160,000 people already rely on it.

Mathcad's the best-selling math software because it gets results. Here's how:

- Easy to learn and use Microsoft® Windows or UNIX interface
- Easy to use symbolic calculations
- Standard Electronic Handbook with hundreds of useful built-in solutions
- Optional Electronic Handbooks available
- Differentials, FFTs, cubic splines, matrices and more
- 2-D and 3-D graphics
- Presentation-quality documentation
- Optional Applications Packs with adaptable templates for Electrical, Mechanical, Civil and Chemical Engineering, Statistics, Advanced Math, and Numerical Methods
- PC DOS and Macintosh® versions also available

NEW Electronic Handbooks available

Free demo disk.

For a FREE Mathcad demo disk, or upgrade information, call 1-800-MATHCAD (or 617-577-1017, Fax 617- 577-8829). Or see your software dealer.

*Electronic Handbooks require Mathcad 3.1 and Microsoft Windows 3.0 (or higher) or UNIX.

1-800-MATHCAD

The answer is Mathcad®

IEEE 20

MathSoft, Inc. 201 Broadway, Cambridge, MA 02139 USA • Phone: 1-800-628-4223 • 617-577-1017 • Fax: 617-577-8829

Australia: Hearne (03) 866 1766; Belgium: SCIA 013/55 17 75; Denmark: Engberg 42 25 17 77; Finland: Zenex 90-692-7677; France: ISE (1) 46 09 24 00; Germany: Softline (0 78 02) 4036; Italy: Channel 02-90091773; Japan: CRC 03-3665-9741; Netherlands: Klaasing 01620-81600; Sweden: AkademiData (018) 24 00 35; Switzerland: Redacom 032 41 01 11; U.K.: Adept Scientific (0462) 480055. In other locations, contact MathSoft, USA.

Circle No. 14

Technically speaking

Fax facts

With more and more inexpensive laser printers available, engineers and other office workers have a veritable printing shop at their disposal. When using word processing and desktop publishing software, they now can choose from dozens, even hundreds, of typefaces or fonts. While few would maintain that character sets with stars, smiling faces, and pointed fingers have made writing more enjoyable, that capability plus the many fonts enable almost anyone to produce high-quality, professional-looking documents in next to no time.

Unfortunately, though this has vastly improved the quality of interoffice birthday announcements, sometimes the quality of facsimile transmissions has suffered. Some typefaces or fonts used in letters may look good on paper but terrible when transmitted. This is because most fax machines scan approximately 203 dots per line by 98 lines per inch (about 4 lines per millimeter), and at this resolution the details of many typefaces can be lost or distorted.

A recent study done by Adobe Systems Inc., Mountain View, Calif., developer of the PostScript printer language, shows how typeface choice can affect the appearance of a facsimile transmission. Adobe found that among its PostScript fonts, Helvetica, ITC Bookman, Lucida, and Palatino maintain their legibility best when faxed. Adobe's top-rated fax font is Lucida, which, however, is seldom part of the font packages included with lower-end printers and so may not be available in some users' offices. But the popular Courier and Times Roman fonts do not fax well, according to the study.

Lynne Garell, corporate type-marketing manager at Adobe Systems, offers some further suggestions for creating faxes that will be legible.

- Use a 12- or 14-point medium-weight font for body text, and steer clear of heavyweight fonts with very thick letters and little space between the legs of the characters. The spaces between the letters can disappear in a fax, leaving long, narrow blobs of ink.
- Avoid using bold face whenever possible because a medium-weight font becomes a heavyweight one when bolded. Exceptions may be made for titles with large fonts, where small distortions will not affect readability. Bold face can be used for emphasis, but this should be done sparingly.
- Use a standard upright font instead of italics. If a line is accidentally distorted during the transmission, italic characters become much harder to read than their straight counterparts.
- And refrain from using Helvetica Narrow or any other condensed font. In a fax, the spaces between the letters of such fonts can also disappear.

Fax Fonts: Recommended

Palatino

Helvetica

ITC Bookman

Fax Fonts: Not Recommended

Downwind

GoodCity Modern Plain

Name this machine

The art of naming technologies can sometimes be as complicated as inventing them. When the now ubiquitous personal computer was readied for its unveiling, the marketeers pulled out all the creative stops in dubbing it the *micro* computer, to denote a size some degree smaller than the behemoths with which the general public was familiar. It did not matter in the least that no relationship existed between the size of the PC and its predecessor; it satisfied the public desire for a high-tech name.

The latest development in computing, the handheld or pocket computer, has until now escaped a "techie" name, but it appears that the time is ripe. While the term *palm-top* has been used to describe these Lilliputian marvels, the name lacks the technical ring that accompanies the debut of many consumer electronics advances. An article earlier this year in *The New York Times* nicknamed them *picocomputers*, in a play on the prefix *micro*. (One wonders what happened to the *nanocomputers*. . . .)

The size of the handheld computers makes them too small for keyboards, and most are operated by using a special stylus to write directly onto the screen. With tweezers in hand, we eagerly await the arrival of the *femtocomputers*.

Quotable quotes

Engineers are often stereotyped as poor communicators. And it's a fact that our technical and specialized language, along with a sometimes unique way of looking at the world and its problems, can make us incomprehensible to many outside the profession. Yet the ability to communicate effectively and clearly is just as vital to an engineer as the ability to do a Laplace transform.

Because universities are aware of this need to improve the communication skills of would-be engineers, many of them now require technical writing courses and/or formal laboratory reports as part of the curriculum.

Such skills do not develop overnight, however. As with any endeavor, mistakes will be made in the learning process—witness the following memorable excerpts from formal reports submitted by electrical engineering sophomores enrolled in their first electrical networks class. The reports concern a simple investigation of resistive-capacitive (RC) networks. The university involved—located in the southwestern part of the United States—has requested anonymity to protect the guilty.

"Stated in layman's terms, the voltage due to a resistor or the current due to a resistor is a constant."

"First and second circuses [read circuits] were reduced to a capacitor and a resistor in this manner."

"We are trying to attain calculations applicable in the free world." [One assumes that the author meant "real" world.]

"The time constant of such a circuit is defined by the multiplicative value of the resistance of the resistor and the capacitance or inductance of the capacitor and inductor consecutively."

"When confronted by a complicated circuit, feelings of panic might arise at the sight of many components connecting to one another; especially, if they are connected to capacitors or inductors."

"An analogy can be made between a tax-

(Continued on p. 15)

Sometimes an opportunity just falls in your lap.

Now the world's most carefully engineered credit card can help you win one of the most useful tools of our time—a Compaq LTE Lite/20 Notebook Computer.

Simply apply for the Institute of Electrical and Electronics Engineers Gold MasterCard® card before December 31, 1992. When your application is approved, you'll be entered automatically in a drawing to win one of these powerful computers.†

And you'll be a winner whether you take home a computer or not, because the IEEE Gold MasterCard offers a host of benefits* designed to give you unparalleled flexibility and value.

- Higher credit lines for IEEE members—up to $50,000
- Purchase protection and extended warranty program
- 24-hour, toll-free Customer Satisfaction
- Common Carrier Travel Accident Insurance—up to $1,000,000 at no additional cost

1-800-847-7378 ext. 5000.

Call MBNA America toll free to apply for the IEEE Gold MasterCard and to get the tools you need to live life to your specifications. Please use priority code KBUN when calling.

†No purchase necessary, see official rules for alternate means of entry.
*Certain restrictions apply to all benefits as described in the brochure that accompanies your access checks.
MasterCard® is a federally registered trademark of MasterCard International, Inc., used pursuant to license.

MBNA AMERICA®

IEEE

OFFICIAL RULES— NO PURCHASE NECESSARY

1. You are entered automatically in "The Great Computer Sweepstakes" when your application for an MBNA® IEEE Gold MasterCard is approved between 5/1/92 and 12/31/92.

2. If your application is not approved, or if you do not wish to apply for a credit card but want to enter the sweepstakes, you can enter by hand-printing your name, address, ZIP code and the words "The Great Computer Sweepstakes" on a plain 3" × 5" piece of paper. Mail your entry to: The Great Computer Sweepstakes, P.O. Box 7467, Melville, NY 11775-7467. Enter as often as you wish, but each entry must be mailed separately and be received by 12/31/92. Mechanically reproduced entries will not be accepted.

3. Grand Prize (3): Compaq LTE Lite/20 Notebook Computer. Winners will be selected in a random drawing from among all automatic and mail-in entries received prior to the sweepstakes end date. Judging will be conducted by National Judging Institute, Inc., an independent judging organization whose decisions are final on all matters relating to this sweepstakes. All prizes will be awarded and winners will be notified by mail. Prizes are non-transferable and no substitutions are allowed. Sponsor and its agencies assume no responsibility or liability for damages, losses or injury resulting from acceptance or use of prize. Taxes, if any, are the responsibility of the individual winners. Winners may be required to execute an affidavit of eligibility and release within 14 days of notification attempt. No responsibility is assumed for lost, misdirected, illegible or late entries or mail. Entry constitutes permission to use winners' names and likenesses for publicity purposes without further compensation.

4. Sweepstakes open to engineers who are residents of the U.S. except employees and their families of MBNA America, MasterCard International, Visa U.S.A., and their divisions, affiliates, subsidiaries, and advertising agencies, and Don Jagoda Associates, Inc. This offer is void wherever prohibited and subject to all federal, state and local laws.

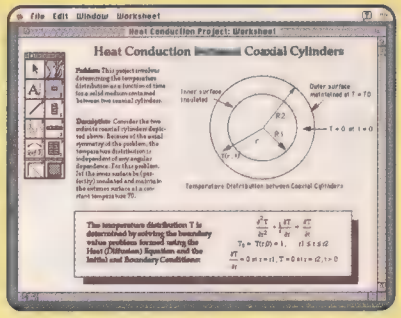
5. For the names of the winners, send a stamped, self-addressed envelope to: "The Great Computer Sweepstakes" Winner List, P.O. Box 7473, Melville, NY 11775-7473.

AD7-34-92

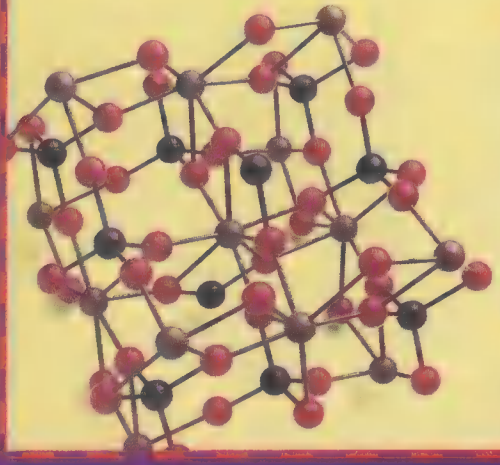
IT'S HARD T

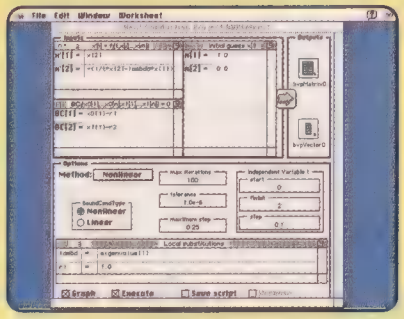
A SINGLE SOFTWARE PROGRAM –

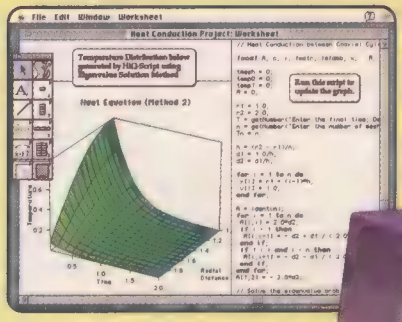
- *Analyzing the Deformation of a Nonlinear Elastic Beam*
- *Performing Linear and Nonlinear Circuit Analysis*
- *Studying the Binding of Antibiotics in the Bloodstream*
- *Modeling a Pumping Heart and Predicting Heart Failure*
- *Analyzing the Structure of White Dwarf Stars*
- *Determining the Shock Waves in Jet Nozzles*
- *Solving Electromagnetic Scattering Problems*
- *Computing the Trajectory of a Spacecraft*
- *Predicting the Levels of Smog Pollution*
- *Solving an Airline Scheduling Problem*



(Top Screen) *HiQ's Project Worksheet interface is a dynamic, interactive, multipage project document. (actual screens)*
(Left) *HiQ's Problem Solvers automatically generate HiQ-Script code along with numerical or graphical results.*
(Right) *HiQ-Script is dynamically linked to HiQ's powerful graphical editor and to all data in the project.*







O BELIEVE...

HiQ™ – CAN SOLVE PROBLEMS LIKE:

FREE DEMO PACKAGE!

Just ask HiQ customers like...

Argonne National Labs
Lockheed Corporation
Dow Corning
Magnavox
National Institutes of Health
NASA
Eastman Kodak
Motorola
General Electric
Exxon Corporation

and a number of leading universities. Here's what they're saying...

"HiQ is... Creating a Revolution for Engineers & Scientists!" – Macintosh Engineering & Science Report

"HiQ is in another league from the other computational programs on the market!" – Jeffrey Kane, M.D., Biomedical Researcher

"It's a flexible environment... HiQ is head and shoulders above what we used in the past..." – Paul Toivonen, Senior Project Engineer, McDonnell Aircraft

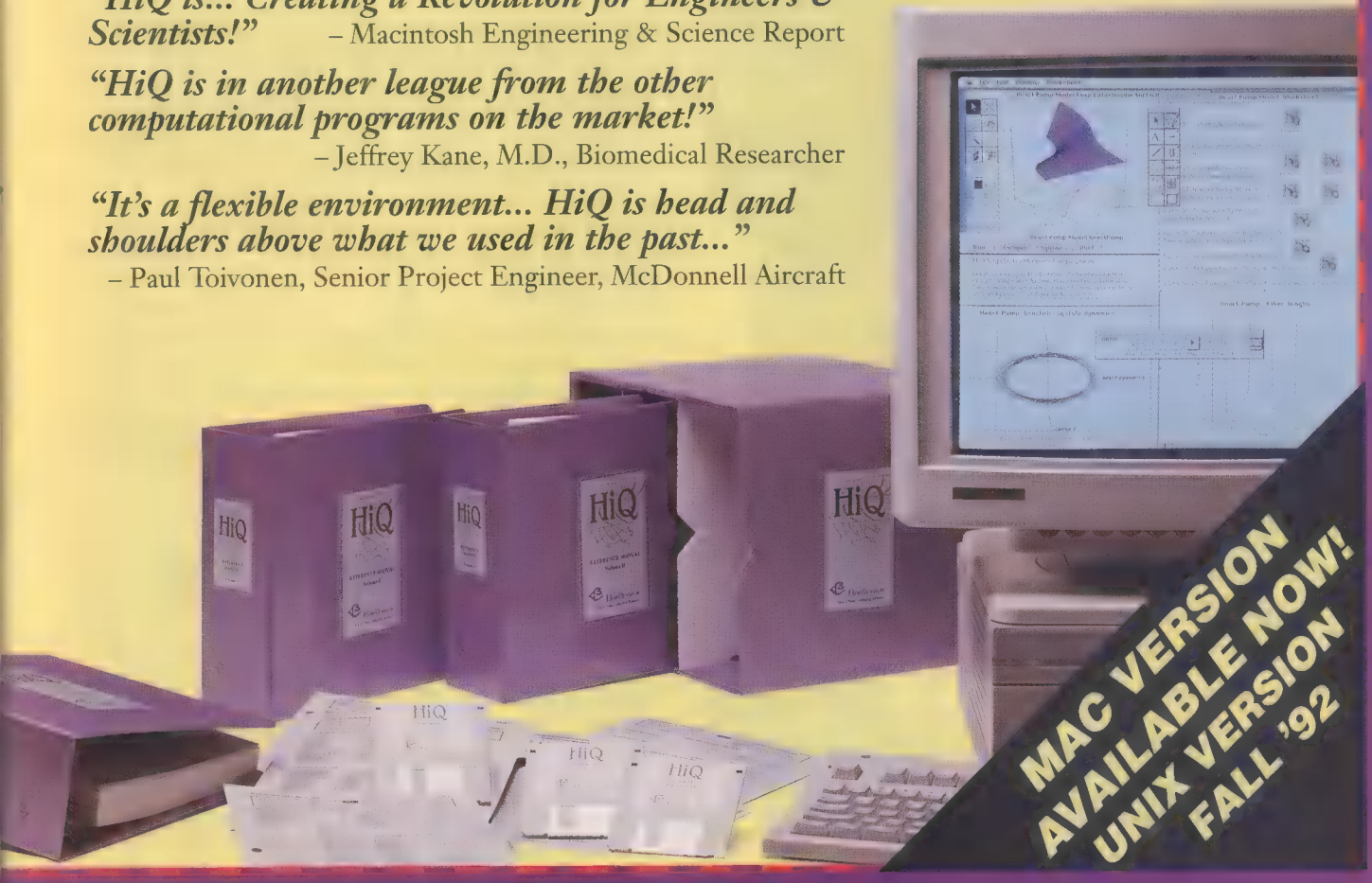
BIMILLENNIUM

First in Power Computing Software

Bimillennium Corporation
101 Albright Way
Los Gatos, CA 95030

Call 1-800-488-8662

Circle No. 26



Calendar

(Continued from p. 8)

Advanced Semiconductor Manufacturing Conference and Workshop (ED); Sept. 30–Oct.1; Cambridge Hyatt Regency Hotel, Cambridge, Mass.; Margaret Bachmeyer, SEMI, 2000 L St., N.W., Suite 200, Washington, D.C. 20036; 202-457-9584; fax, 202-659-8534.

Challenges in Optoelectronic Packaging (LEO, CHMT); Sept. 30–Oct.1; Hyatt Regency Hotel, Baltimore, Md.; IEEE/LEOS, 445 Hoes Lane, Box 1331, Piscataway, N.J. 08855-1331; 908-562-3893; fax, 908-562-1571.

Fourth Annual IEEE International Workshop on Computer Aided Modeling Analysis and Design of Communication Links and Networks (COM); Sept. 30–Oct.2; Le Chateau Montebello, Montebello, Que., Canada; Hussein T. Mouftah, Department of Electrical Engineering, Queen's University, Kingston, Ont. K7L 3N6, Canada; 613-545-2934; fax, 613-545-6615.

International Professional Communication Conference—IPCC '92 (PC); Sept. 30–Oct. 2; La Fonda on the Plaza Hotel, Santa Fe, N.M.; Susan Dressel, Information Services, Los Alamos National Laboratory, Mail Stop M704, Los Alamos, N.M. 87545; 505-667-6101; fax, 505-667-1754.

International Workshop on Hardware–Software Codesign (C, CAS); Sept. 30–Oct. 2; Holiday Inn, Estes Park, Colo.; IEEE Computer Society, Conference Department, 1730 Massachusetts Ave., N.W., Washington, D.C. 20036-1903; 202-371-1013; fax, 202-728-0884.

OCTOBER

International Workshop on Intelligent Manufacturing Systems (CS et al.); Oct. 1–2; Hyatt Regency Hotel, Dearborn, Mich.; N.A. Kheir, Oakland University, Dodge Hall of Engineering, Rochester, Mich. 48309-4401; 313-370-2245; fax, 313-370-4261.

GaAs Reliability Workshop (ED); Oct. 4; Fontainebleau Hilton Hotel, Miami Beach, Fla.; Anthony Immorlica, General Electric Co., Electronics Laboratory, Electronics Park, Syracuse, N.Y. 13221; 315-456-3514; fax, 315-456-0695.

(Continued on p. 70D)

Technically speaking

(Continued from p. 14)

payer and a seemingly sophisticated circuit as in the case of the movement of money between the government and the taxpayers. Once the tax is paid by citizens, the government utilizes that money by pumping it back into the economy by creating jobs or programs. The taxpayers are then working to earn that money back. This creates a continuous circling of the tax money. In the same manner, the RC circuit can be analyzed by the capacitor charging all the voltage and then discharging it through a resistor."

"From the point where this voltage stroked the curve, we drew a vertical line to the time scale."

"Some small differences between the evaluated values and the theoretical values were found. However, these discrepancies were below the average of 30 percent. So, it can be said that these experimental values were fairly within the acceptable range."

"LC circuits are handled differently. Some, because there exists a contradistinction in the mathematics."

"In the LC circuit, there is no resistor to dissipate energy; therefore, the input is not altered by the circuit."

More on that misnomer, power supply

The discussion of the term *power supply* in last November's *Technically Speaking* column [p. 18]—and the suggestion there in a letter from reader Victor Wouk that the term *power converter* would be more appropriate—got Michael Robinson of San Jose, Calif., to thinking why the term *power* should be used at all. Power is energy used per unit time, he pointed out, so what would a supply of energy per unit time be?

As an analogy, Robinson noted that his home is connected to the municipal water supply, not to the municipal water flow supply (which refers to the supply of water per unit time). Therefore, he wondered if the argument about the term *power supply* should really be about *energy supply.*

What is commonly called a *power supply* is not a supply of anything, either power or energy, but a converter, Robinson wrote. So is a solar panel, which converts solar energy into electricity, and a battery, which converts chemical potential energy into electrical energy. Any device that, like a battery, can convert potential energy into electrical energy can be used as a storage device.

Is the difference (between something which is a *supply* and something which is not) the capacity for storage? Robinson asked. If not, then it must have something to do with the act of creation. His bank account is a storage device for money, but he would not think of it as a money supply, he said. Very few things would actually be energy supplies—the sun, perhaps, although Robinson said an office mate argued against that on the ground that matter and energy are the same.

Looking in the American Heritage dictionary, Robinson found that the primary definition of supply is to make something available for use; having a store or stock of something is considered a less important meaning. A supermarket could, therefore, be said to supply food, although it does nothing but pass food on from producer to consumer.

And concluded Robinson: "Since a *power supply* makes electricity available for use (try running a system without one), it is in fact a supply. But then would it perhaps be better to call it an *energy supply?*"

Spectrum *magazine welcomes letters from readers prompted by items in the* Technically Speaking *column. Send them to Managing Editor,* IEEE Spectrum, *345 E. 47th St., New York, N.Y. 10017; fax: 212-705-7453.*

COORDINATOR: Kevin Self
CONSULTANT: Anne Eisenberg, Polytechnic University

For High Temperature Superconductor Answers, Go to the Source.

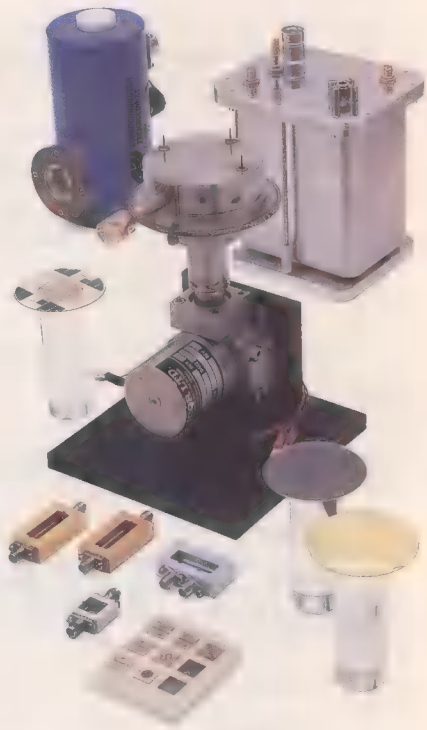
Q: Are the new superconductors really practical for electronic devices?

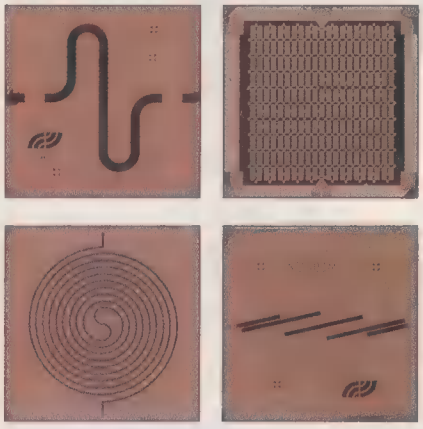
A: "YES, and they can give a significant performance advantage to your systems. At SUPERCONDUCTOR TECHNOLOGIES INC. (STI), the new high temperature superconductors (HTS) have developed rapidly, especially for microwave applications. Our high quality superconducting thin films, which have losses *100 times* lower than copper or gold, can be patterned into thin-film circuits with Qs as *high* as *30,000*. In fact, STI now provides a range of products that give extraordinary performance advantages to a number of industries.

"STI is now working with the microwave industry in an aggressive program to develop superior passive components with HTS. This includes resonators, filters, oscillators, delay lines and subsystems. In addition to HTS films, we provide custom HTS circuits, components and assemblies. And our HTS circuit fabrication department builds customers' designs from mask making to packaging.

"HTS theory is now HTS reality. Managers and systems engineers in a growing number of industries now have the opportunity to use the performance advantages of high temperature superconductors."

Jim Bybokas
Vice President
Superconductor Technologies





Examples (shown approximately 2X actual size) of custom HTS circuits include microstrip resonators, coplanar delay lines, lumped element inductors and microstrip filters.

STI has been awarded more than 20 development contracts and has recently completed a major three-year program for DARPA to develop HTS materials and devices for microwave applications.

At STI, we have successfully developed HTS materials with transition temperatures over 100°K. As we advance the state of superconductor technology, we're continually adding innovative new products to the marketplace.

Make high performance HTS an integral part of your component and system development now by making STI part of your development team. For more information, call Jim Bybokas, Vice President of Product Development at Superconductor Technologies Inc., at (805) 683-7646. Or write him at 460-F Ward Drive, Santa Barbara, CA 93111-2310… FAX (805) 683-8527.

You'll be surprised at what has been accomplished with high temperature superconductors!

SUPERCONDUCTOR TECHNOLOGIES

Your complete HTS source.

Circle No. 22

AUGUST 1992 Volume 29 Number 8

Higher grades for accreditors?

After years of considered discussion accompanied by some emotion, it appears that undergraduate-engineering curricula are going through the first stages of a metamorphosis.

A strong driving force has been the general agreement that design has been given short shrift in the traditional engineering curriculum.

But as experimental curricula and even major permanent changes are contemplated, educators are speculating about the role of the Accreditation Board for Engineering and Technology (ABET) in abetting such developments. Some have felt the board has in past years been less than enthusiastic about encouraging innovation.

John Prados, president of the ABET and a professor of chemical engineering at the University of Tennessee, admits that while the ABET has focused on serving the student and the employer, it has not adequately attended to the concerns of the engineering schools themselves. Schools need help in shaping their programs and continuously improving the quality of education they provide, he notes.

The ABET has been criticized for excessive rigidity in interpreting its accreditation criteria, including the design requirement, Prados said, a sentiment underscored in a report in 1991 of the ABET/Engineering Deans Council Liaison Task Force.

But, in fact, proposed changes in how engineering programs in the United States would be accredited were drafted for the ABET board of directors in 1990, and will be voted upon by the board in October. The proposals are aimed in part at encouraging innovation.

One example is the design requirement. Whereas the criteria for it now center on devoting a half year of 16 semester-hours to design, the new criteria would play down the quantitative aspect (number of hours) of a design program and play up its quality.

The draft proposal intentionally omitted the existing metric requiring "at least one course which is primarily design, preferably at the senior level . . ."

It would replace that metric with a requirement that each program

> "must include a meaningful, major engineering design experience that builds upon the fundamental concepts of mathematics, basic sciences, the humanities and social sciences, engineering topics, and communication skills. The scope of the design experience within a program should match the requirements of practice within that discipline. The major design experience should be taught in section sizes that are small enough to allow interaction between teacher and student. This does not imply that all design work must be done in isolation by individual students; team efforts are acceptable where deemed appropriate. Design cannot be taught in one course; it is an experience that must grow with the student's development. A meaningful, major design experience means that, at some point when the student's academic development is nearly complete, there would be a design experience that both focuses the student's attention on professional practice and is drawn from past course work. Inevitably, this means a course, or a project, or a thesis that focuses upon design. 'Meaningful' implies that the design experience is significant within the student's major and that it draws upon previous course work, but not necessarily upon every course taken by the student."

Prados thinks that undue restraints are placed on curricular innovation by the preoccupation of some accreditation teams with a minimum metric, and he favors its replacement with the holistic, if less specific, approach outlined above.

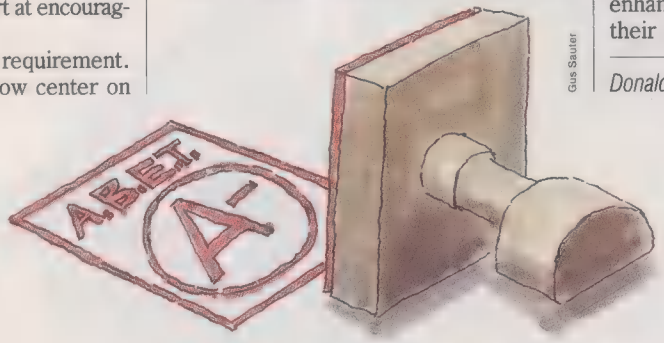
He and other proponents would rather have innovative programs evaluated qualitatively to enable evaluators to focus on the coherence and effectiveness of the design experience and not be distracted by excessive concern with quantitative requirements.

On the other hand, some evaluators and some schools worry that the absence of a quantitative minimum design content could make it difficult to reach and defend accreditation judgments, and would encourage inconsistency among evaluation teams. ABET participants in certain engineering disciplines (excluding electrical engineering) have reacted to this concern by proposing that a quantitative design requirement (usually 16 semester-hours) be added to the program criteria for their specific disciplines.

Such concessions aside, those who support the changes embodied in the ABET proposals feel that the engineering education community must shift its focus in evaluating educational programs toward assuring quality and away from inflicting punishment on those programs that do not conform to rigid specifications.

Such shifts in emphasis by the ABET should help faculties who are well along in revamping their undergraduate curricula to enhance and extend the design content of their new programs.

Donald Christiansen



Gus Sauter

DATA SECURITY

Last November—amid carefree, swimsuit-clad escapees from the first blasts of winter up north—a justifiably somewhat paranoid group convened at the Fontainebleau Hilton in Miami Beach, Fla. While waiting for their symposium to start, attendees traded business cards from more than 1000 organizations, including the U.S. Central Intelligence Agency, Del Monte Tropical Fruit, the Colorado Lottery, Saudi Aramco, Pillsbury, the World Bank, Brooklyn Union Gas, Boeing, Maytag, the California State Automobile Association, Coca-Cola, Blue Cross & Blue Shield, Sony, Lockheed Missiles & Space, Campbell Soup, Dow Chemical, Florida Department of Corrections, Exxon, London Life Insurance, Sara Lee, Texas Department of Mental Health and Retardation, AT&T, Ralston Purina, IBM, and Domino's Pizza.

This cross section of contemporary working society, from cake makers to Star Wars designers, was present to discuss a pressing, common concern. From the podium, the opening speaker's voice boomed a loud warning: "We've got a problem out there, folks—it's called personal computers!"

That speaker—Tom Peltier, then manager for computer security at General Motors Corp.—found no dissenter among the crowd. They were not modern-day Luddites but, like himself, corporate information security specialists. To many of them, the halcyon days had been the era of the mainframe, when limited access and strict quality assurance controls on software made security concerns seem, in retrospect, relatively minor. Now, PCs and networks are giving them nightmares, and such advances as greater speed, connectivity, and accessibility, only add new horrors.

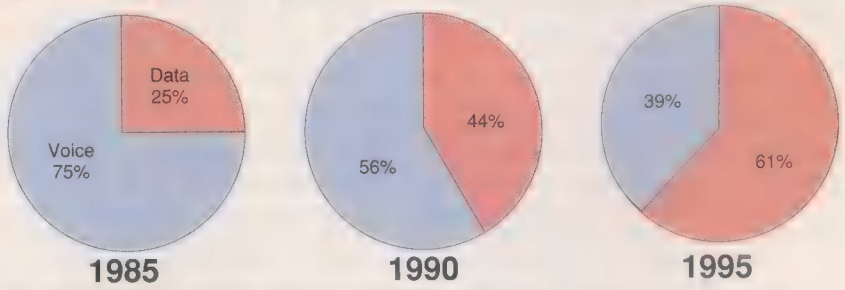
Of course, the benefits of being hooked up are so dazzlingly apparent that communication lines are increasingly abuzz with data, images, and other digital information [Fig.1]. But despite a few well-publicized intrusions and virus incidents, the security risks of modern computing are all too often ignored. True, the loss of information to accidental errors remains the leading risk to computer security today. But in speaking to the U.S. Congress recently, John W. Lyons, director of the U.S. National Institute of Standards and Technology (NIST), Gaithersburg, Md., observed that "intentional abuses to sensitive information, such as industrial espionage, are now becoming important enough to cause national concerns."

The United States for one should worry. Every day $1 trillion or so is electronically transferred among U.S. banks. The Bank of America alone processes 10 000 new accounts each day, and "smart criminals will come in and open an account" in order to steal money, said Donald Parrot, an assistant vice president in charge of retail automation at the San Francisco–based bank. Robbers can steal more with computers than with a gun; terrorists could do more permanent damage with a keyboard than a bomb—and without ever crossing an international border. In many cases, crimes committed by remote control escape notice and when spotted, are tough to trace.

Other highly likely targets are R&D-intensive companies, because their proprietary information has such a high content of valuable intellectual property. More recent

John A. Adam Senior Associate Editor

Data drowning out voice



[1] For the 1750 business networks tracked by Vertical Systems Group in Dedham, Mass., increased use of computers is changing the traffic mix. Today, 54 percent of their bandwidth is allocated to data; voice still dominates the public (phone) network.

Defining terms

Audit trail: the results of monitoring and keeping track of each operation on objects; for example, an audit trail might be a record of all actions taken on a sensitive file.

Bacterium: a stand-alone program that repeatedly replicates itself and, by its sheer numbers, takes over a system.

Checksum: digits or bits summed according to arbitrary rules and used to verify the integrity of data; for example, a checksum operation may result in a 64-bit number being appended to a long message, so that a change in the message would change the number.

Computer virus: a small, and unwanted, program that replicates and attaches itself to other programs in the system.

Digital signature: data that can be generated only by an agent that knows some secret, and hence is evidence that only that agent must have generated the data.

Information: data to which meaning is assigned, in accordance with the context and assumed conventions.

Integrity: the property that an object is changed only in a specified and authorized manner. Data integrity, program integrity, system integrity, and network integrity all have relevance to information security.

Intruder: an unauthorized user who gains access to a computer system to examine data and use the system for his or her own purposes.

Logic bomb: code planted in an otherwise legitimate program that is not executed until some predefined trigger condition occurs, at which time it damages the system by erasing or corrupting files or causing it to "crash."

Public key encryption: an asymmetric scheme that uses a pair of keys. For encryption the public key encrypts data and a corresponding secret key decrypts it. For digital signatures, the process is reversed: the sender uses the secret key to create a unique electronic number that can be read by anyone possessing the corresponding public key in order to verify that the message is truly from the sender.

Secret key encryption: the traditional scheme, where only one key, known to both the sender and receiver of a message, is used to encrypt and decrypt the message. Also known as symmetric or private key encryption.

Trigger condition: an external event that causes a program to change its behavior.

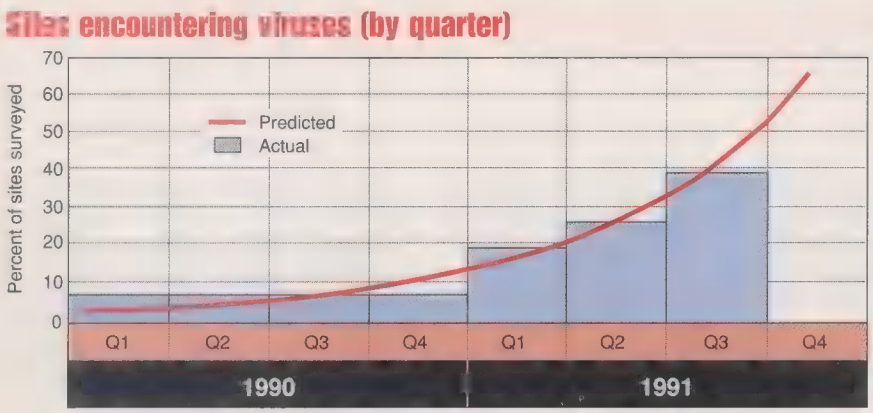
Trojan horse: an apparently useful program containing hidden code that either executes malicious acts when triggered by some external event or provides a trap door through which an intruder can surreptitiously access the system.

Trusted system: a system believed to enforce a given set of attributes to a stated degree of assurance.

Worm: a self-replicating program that moves from one system to another along a network.

Photo: Jim Pickerell

0018-9235/92/$3.00©1992 IEEE



[2] Results of a survey of 602 companies with 100 or more personal computers each (an average of 1002 PCs per company) by Dataquest Inc., San Jose, Calif., show that the number of organizations experiencing at least one virus incident during a quarter is growing rapidly.

concerns are network vulnerability and, for personal computers, infection by viruses.

The rate at which companies are encountering viruses is growing, but how fast is debatable. Certus International Corp., Cleveland, Ohio, believes that data from a survey [Fig.2] by Dataquest Inc., San Jose, Calif., suggests growth this year will be exponential. On the other hand, data derived independently by IBM Corp., Hawthorne, N.Y., suggests that the virus incident rate per 1000 PCs was 1.1 during the fourth quarter of 1991, and has been growing at a linear rate over the last two years.

But regardless of the rate of increase, no one denies that virus encounters are on the rise. Compounding the threat is the fact that both network intruders and virus writers are growing ever more devious, according to authorities in industry, on computer emergency response teams, and at the U.S. Federal Bureau of Investigation. A case in point is their creation of new, polymorphic viruses that can spawn billions of variations of themselves, which forces a reexamination of the basic methods employed by antiviral software.

Similar developments are occurring in network security. The Computer Emergency Response Team based in Pittsburgh, which helps the administrators of about a million host computers on the Internet, is starting to see some "automated attacks." These involve knowing a system's weaknesses so well as to be able to rehearse and program an attack on them. First, a number of addresses might be winnowed to find common vulnerabilities. Then, password files might be downloaded and cracked off-line to penetrate the host computer. After a rehearsal, the cracker actually logs in and uploads his automated attack program, then signs off. In a few days, he or she may log on again to harvest what information has been gathered, said Ed DeHart, director of the seven-member Computer Emergency Response Team. With less time logged in than with manual cracking, the intruder lessens his odds of being discovered. A 1991 report by the National Research Council (NRC), Washington, D.C., warns against exotic "tunneling attacks," which take advantage of a weakness intrinsic in a system at a fundamental level and not apparent during testing or design. (For instance, rather than attempt to break an encryption scheme, an attacker might find a way to modify the code of a processor used to encrypt data.) Such concern, the report said, might preclude the use of foreign components or those made by commercial rivals.

When all is said and done, the technical measures needed to keep information secure may not be worth the expense. They must be weighed against other factors, such as the risk that employees will be bribed for information. In any case, high-grade attacks become continuously more ingenious, and for many organizations, it may be better to avoid an endless escalation of costly countermeasures and concentrate instead on recovery rather than prevention. "Security does not make you $1 on the bottom line," said A. Padgett Peterson, an engineer who nevertheless helped convince managers at Martin Marietta Corp. to back a comprehensive security program.

> A terrorist can do more damage with a keyboard than a bomb—and never cross an international border

The insidious advances made by malicious hackers, and some current and future means of prevention, are examined in the first part of *IEEE Spectrum*'s report, "Threats and countermeasures" [pp. 21–28]. As *Spectrum*'s report points out, there are many degrees of protection to be had almost for the asking. Many of the solutions cost little and many of the services are still free.

The second article, "Cryptography = privacy?" [pp. 29–35], examines concerns about the main encrypting and enciphering schemes being proposed as a way to ensure data security. The use of crypto-algorithms is assuming new importance to both communications and computer security. Here the interests of government intelligence agencies and private groups often collide, as evidenced by the controversy over the Digital Signature Standard proposed by the U.S. National Institute of Standards and Technology. (A revised version is being made public this month.)

Included in this segment is a lengthy response by the U.S. National Security Agency (NSA) in Fort George G. Meade, Md., to questions posed by *Spectrum*. Following NSA's statements, which address both the security of the new cryptographic algorithm and the status of export controls, are critiques by Ronald L. Rivest, a computer scientist at the Massachusetts Institute of Technology, Cambridge, and D. James Bidzos, president of RSA Data Security Inc. in Redwood City, Calif.

"Bad code," a tutorial on viruses, worms, bacteria, and other computer diseases, forms the third part of this report [pp. 36–40]. It describes how experts classify the various forms of malicious code at work today, the ways in which they hide and work their mischief, and a few of the infamous incidents—such as the attack on the Internet network, in the fall of 1988, of a worm program that devoured massive amounts of CPU time—that have gained international notoriety. Authors John B. Bowles and Colón E. Peláez of the University of South Carolina also discuss some of the basic forms of prevention and cure and, in an aside, provide a brief overview of the origins of virus and worm nomenclature.

A discussion as to whether data security should be regulated, and if so how, in the article entitled "A security roundtable" concludes this report [pp. 41–44]. For this exchange, experts from throughout the world were convened digitally, using electronic mail over the Internet. They were Klaus Brunnstein of the University of Hamburg in Germany; William J. Caelli of Queensland University of Technology, Australia; and in the United States, Lance J. Hoffman of George Washington University, Peter G. Neumann of SRI International, Marc Rotenburg of Computer Professionals for Social Responsibility, and Willis H. Ware of Rand Corp.

Together, they examined some interrelated aspects of the security and vulnerability of computer systems, the electronic building blocks of the information age. Several of the international authorities who took part said the situation is reaching crisis proportions. An issue was whether software is a unique product and needs special treatment, like that accorded some other government-regulated industries. ✚

Threats and countermeasures

Computer viruses and network attacks are becoming quite sophisticated. Will current precautions or those in development work?

After enthusiastically laying down computer networks and private telecommunications systems in the 1980s, many organizations are now afflicted with "information insecurity"—electronic data vulnerable to interception or corruption.

"All that investment is already made and they find out it's not secure," said Morgan E. Death, general manager for Hughes STX Corp. in Vienna, Va. An information security company formed in 1973, STX was acquired by Hughes Aircraft Co., Los Angeles, last October, and a month later, its giant parent, General Motors Corp., declared information security to be one of the company's top priorities.

The security issue extends beyond companies, of course—to medical records, military plans, phone conversations, financial transactions, and even an individual's tastes in videos. These are examples of information that many diverse parties—government, industry, and individuals—often want to keep secure, ensuring both integrity and privacy.

Much of the threat to information security is the traditional one of electronic spying, such as picking up electronic emissions from individual computers or from transmissions between physical locations. But recent problems with computer viruses and network attacks add a new dimension, whereby data, rather than merely being passively intercepted, may be actively destroyed or corrupted. It is this area that *IEEE Spectrum* focuses on in what follows, examining the threats and some possible remedies.

STRAINS OF VIRUS. Electronic infection is a rather recent—hence immature—development that began in the later 1980s. Today there are many classes of viruses, and they sometimes combine characteristics, such as stealthiness and polymorphism. [A sampling of the main innovations in viruses appears in the table on p. 25.]

John A. Adam Senior Associate Editor

Hundreds of "new" viruses have been appearing each year, mostly from Europe. The main targets are the several tens of millions of IBM-compatible personal computers to be found around the world. But antidotes are usually possible.

At present, there are perhaps 1350 viruses affecting IBM-type PCs, more than 200 Amiga viruses, and some 35 Macintosh viruses. There are also some Unix and several mainframe viruses, most of which are test versions that "hopefully were eradicated by security wizards," said Klaus Brunnstein, a professor at the Virus Test Center at the University of Hamburg in Germany. The center analyzes most new viruses, with help from Germany's information security agency in Bonn and from the MicroBIT Virus Center at the University of Karlsruhe.

Brunnstein estimated that new viruses appear at the German test centers at a rate of 10 per week, but not all are "in the wild," that is, viruses released by malicious hackers to do harm. Companies may write viruses to test security programs, and virus writers often send new codes to the antiviral research community both as a courtesy and intellectual challenge. Since most virus authors, however, merely adapt or "patch" existing virus programs, only about 300 basic virus families exist so far, according to Brunnstein.

Although there are some useful applications of viruses and worms, better known are the malicious bits of compact code. The most common virus is Stoned, the bane of IBM-type personal computers, whose lineage traces to New Zealand in early 1988. At first, Stoned was mainly a nuisance, displaying "Your PC is stoned!" at boot time. Then options were added. One of the more recent of 26 derivatives of Stoned, with the destructive capability of overwriting hard disks, is the Michelangelo virus that captured media attention last March.

A current variant, called Stoned III, epitomizes a first-generation class of so-called stealth viruses. Martin McKee, a graduate student in computer science at George Washington University (GWU), Washington, D.C., has just completed an analysis on Stoned III, which first appeared on the GWU campus in February. "Its installation code is very similar to that of the Stoned virus," he said. "It uses the same clumsy memory acquisition technique as Stoned, so it inherits the same detectability in this area."

But once Stoned III infects a hard disk, its stealth feature thwarts attempts at detection. McKee disassembled the code (which in general was more tightly written than the original) and found that the stealth feature comprised only 36 bytes. If the code senses that the hard disk master boot record is trying to be read (by antiviral software, for instance), the virus temporarily substitutes a clean copy of the master boot record instead. "The stealth feature by no means makes the virus undetectable, but it can add some difficulty," concluded McKee [a tutorial on viruses appears on pp. 36–40].

CHANGING IMPRINTS. Another new class of virus infection, so far rare in the United States, is the polymorphic virus, so named by antivirus researchers because of the virus' changing imprint. These polymorphic codes are "just becoming the next real problem," said Brunnstein.

Traditional antiviral software, dependent on scanning for a virus' known signature, is ineffectual against this new breed of virus because the polymorphic code has a different signature each time it is encrypted. Scanners usually rely on 16–32-byte search patterns to detect known viruses.

Random number generators in polymorphic viruses can alter the pattern in the key stub of a virus by inserting junk code, changing the order of significant bytes or their location in registers. So antivirus writers are developing algorithmic software that searches not for certain header lengths or instructions but for patterns critical to the virus' operation.

Hamburg's Virus Test Center recently began performing experiments on this new potential plague to see how effective some of the antidotes might be. According to Brunnstein, the problem is that even the presently rather simple codes can be astoundingly prolific.

Causing a lot of recent concern is an add-on module of about 3000 bytes known as Mutating Engine 0.9/0.91, a tool created by a Bulgarian virus writer called Dark Avenger. With its built-in random number generator, the module can produce a virus that has billions of distinct mutations. Currently, just four nonstealth viruses—Pogue Mahony, Dedicated, Fear, and Questo—use this Mutating Engine tool.

Of this multitude of mutations, only a small subset has been analyzed so far. David

0018-9235/92/$3.00©1992 IEEE

M. Chess, a researcher at IBM's high-integrity computing center in Hawthorne, N.Y., generated 5 million variations but has not compared them.

Brunnstein's group in Hamburg generated about 10 000 mutations, only four of which turned out to be twins. The group then tested new algorithmic antiviral software developed by software designers John McAfee, Fridrik Skulason, and Alan Solomon. In this test, McAfee detected all but four mutations; Skulason found all but 13; and Solomon's software, after repeated runs, detected all but one form.

"At first view, this seems excellent," said Brunnstein, who is also a professor of informatics at the University of Hamburg. But, he added, a detection accuracy of 0.01 percent means that many variations may still exist.

Perhaps the scariest point about the polymorphism was reported by Solomon during a June virus conference in Washington, D.C. He suggested that the polymorphism can represent an accelerated type of Darwinian natural selection in which antiviral products weed out all but a few mutations—but those few hardy survivors proliferate.

However, proper implementation of existing methods could curb such polymorphic infections even with imperfect antiviral software. For instance, if antiviral software notes that 27 files are infected and an integrity management system notes that five additional files have been altered, then one can assume 32 files are infected and replace them with backups, noted A. Padgett Peterson, a security manager for Martin Marietta Corp. in Orlando, Fla.

Still, because polymorphic viruses are uncommon and antivirus software has already been written, IBM's Chess believes that "at the moment, [they] are less of a problem than your hard disk crashing."

VIRAL COLLEGES. Authors of viruses do not write them all from scratch. Most antiviral writers would agree with software designer Solomon, who believes "the technology of writing difficult viruses is spreading," mainly because of Virus Exchange Bulletin Boards.

The so-called VX boards are most prevalent in the United States where some dozen exist, offering at least 400 viruses, said Joseph Wells, a virus specialist at Certus International Corp., Cleveland, Ohio. Similar boards are used in Bulgaria, Italy, Germany, and the United Kingdom.

One of these VX boards, the Hell Pit, queries a prospective user on how he heard about the network. Access is granted after

Swat teams on 24-hour call

"We all have wonderful war stories to tell about being roused from sleep," said Barbara Fraser, one of seven members of the Computer Emergency Response Team (CERT). Most computer crackers, like common robbers, prefer to break in during off-hours, she said, and international incidents add to the 24-hour nature of the job. Mostly, however, CERT's business is conducted between 7:30 a.m. and 6 p.m., Pittsburgh time.

CERT's domain is the Internet, a worldwide supranetwork with perhaps a million host computers and five to eight million users. Roughly half are in the United States, and membership is expanding fast in Europe, the Pacific Rim, and South America.

Each day, the CERT team responds to an average of 300 hotline calls and electronic mail messages, most in English. Last year, they averaged about one "incident" a day. Now it is up to three. (An incident is an actual or attempted intrusion.)

They have responded to serious attacks from Europe ("This is NOT A PRANK"), put out a major U.S. hacker alert that counseled "Caution (not panic) is advisable," and warned against electronic mail Trojan horses that cadge passwords from gullible users.

When a call or message comes, the CERT member on duty supplies technical guidance to the site so that they can fix the problem and assess damage. Unless otherwise agreed to, everything is confidential and may even be anonymous. CERT members determine whether the host was networked, its level of security, the system configuration, and whether the system's vulnerability is familiar or new.

CERT director Ed DeHart stresses that any tip is welcome. Last year, for instance, a person reported a failed attempt to seize his password file. CERT went back to the originating site and found intruder(s) "were trying to break into thousands of systems." The originating site alerted management, cut connections to the outside temporarily, and closed the "holes" in its security system.

CERT does not investigate intrusions with an eye to criminal prosecution, but it does recommend whom to contact for investigations by law enforcement groups such as the local police, the Federal Bureau of Investigation (FBI), or the Secret Service.

Most of CERT's traffic consists of security chatter; experts call to share information while others ask about CERT advisories or request general advice. Less often, CERT has to tip off organizations about likely penetrations. "Almost always, an incident is not stand-alone," said Fraser. It may vary from 10 hosts at a single site to "tens of thousands of hosts over the world."

Many people do not wait for a problem but call CERT for a "sanity check"—reassurance that their site and its systems are safe. Novices are not discouraged. "We hold their hands," Fraser said. Help is free and is even encouraged.

CERT was formed only weeks after the paralyzing 1988 attack on Internet by Robert Morris Jr., son of a computer security scientist. It is funded by the Pentagon's Defense Advanced Research Projects Agency through the Software Engineering Institute at Carnegie Mellon University in Pittsburgh.

With its expertise in system vulnerabilities, CERT is expanding its efforts in education and training as well as research and development for network security. Already, it sends a security checklist to sites as needed and advises scores of Unix software vendors of security flaws that need patching. It also keeps a confidential mailing list of vendors regarding vulnerabilities in their products. "This is not the textbook type of security problem," DeHart said. "This is based on what people are doing."

Such companies as Sun Microsystems and NeXT, and more recently IBM, are mentioned a lot in the CERT advisories, noting fixes to system flaws. Rather than being an embarrassment or indictment of their products, this shows that these companies are committed to security, DeHart said.

CIAC (for Computer Incident Advisory Capability), a sister group of CERT with responsibility for Department of Energy computers, is located at the Lawrence Livermore National Laboratory in Livermore, Calif. Known for its software analytical capabilities, CIAC keeps 20–30 viruses in isolation "for dissection and reverse engineering."

Steve Mick, CIAC project leader, said they average perhaps one or two incidents a week. Like CERT, they always wait until a patch is found before they announce the vulnerability. The flaw is described over e-mail as vaguely as possible to thwart would-be crackers. But sometimes, he said, "it's like trying to describe a hula hoop without moving your hand."

Other countries are responding, too. In 1990, Germany's information security agency created two national incident response teams: the Virus Test Center at the University of Hamburg and the MicroBIT Virus Center at the University of Karlsruhe.

The Hamburg center has five staffers and many students who analyze viruses and monitor activities of the German hackers known as the Chaos Computer Club. The center receives 20–100 reports on virus cases each week from Germany and Scandinavia, divided equally between government, industry, and academia. E-mail links aid coordination with other experts in Australia, Europe, Japan, and the United States. A current European Community initiative would create several more CERT-like groups in diverse countries.

All told, the U.S. Department of Justice reports there are more than a dozen CERT teams. Not to be left out, its own FBI recently formed the Computer Analysis and Response Team (CART), which will take its place beside other FBI laboratories, like those for analysis of DNA, chemicals and poisons, and shoe- and tireprints.

Initial plans call for a staff of 12 agents. CART's main task will be the forensic examination of computer evidence, according to manager Stephan McFall. They must also guarantee (somehow) to the satisfaction of U.S. courts that magnetic data has not been altered or deleted since being confiscated. McFall declined to give more details other than to say that research is being done and that CART will also help train agents in the field.

There are so many CERT-like groups in government and industry today that in 1990 the Forum of Incident Response and Security Teams (First) was born. The group meets regularly and organizes workshops on incident handling. Even organizations without worm-busting squads can join if approved. The U.S. National Institute of Standards and Technology [see To probe further, p. 44] has more information.

—J.A.A.

typing in "Todor Todoruv," the name of a Bulgarian VX board operator. Once in, a user can download any number of viruses—including stealth and polymorphic varieties—for Macintoshes, PCs, and so on. Users can also obtain tips on hacking, including password postings, and files such as fraudulent credit card numbers.

Wells calls the VX boards "underground universities." Not only do they serve as training grounds for new hackers, but they are also the means by which new viruses are now released into the wild much faster—to the dismay of antiviral researchers. Wells is discussing the possibility of restricting VX boards with U.S. Federal officials (a difficult task because of freedom of speech issues).

Yet, attempting to control the quantity and quality of such viruses is like facing an accelerating arms race. Current antiviral software is always playing catch-up, needing constant upgrades. For instance, the latest upgrade of the popular F-Prot antiviral product, developed by antiviral writer Skulason, and released in June, detects and removes 72 more viruses than its March version did; in addition, 21 other viruses can now be detected but not removed.

The fee for such software depends on the number of computers involved. It costs US $0.50 per computer for organizations with 2500 to 5000 computers. A year's worth of upgrades is included for a slightly higher price.

Fortunately, in this virus and antivirus arms race, a lot of the viruses tend to be annoying rather than destructive. Also, specific commercial software packages have not generally been targeted to date. Many vulnerable realms have yet to be affected.

For one thing, no virus yet exists that can hop across from Macintosh to IBM systems or IBM to Unix systems. And there have been relatively few examples of "hybrid malware," as Brunnstein put it, in which rogue network software, such as worms or chain letters, transports viruses or Trojan horses in inhomogeneous networks.

Some viruses are mere irritants, displaying messages such as "Find Me," creating images like a starry sky, or playing music like Yankee Doodle Dandy at 5 p.m. every day. More malicious code in the field overwrites hard disks (on all tracks), steals passwords, or swaps names of the computer's filing structure.

Few viruses so far home in on commercial packages, but one that does is the dBASE virus, which corrupts data in the common Ashton-Tate (now Borland) program. "Viruses that attack specific software labels or packages are a relatively new weapon in the hands of the commercial saboteur," said Edward Wilding, editor of *Virus Bulletin*, in Abingdon, Oxfordshire, United Kingdom. Viruses that move decimal points and create other spurious data are a probable future threat, he added.

Hardware-destroying viruses are rare, although a few indirect effects, such as head crashes or printer problems, have been observed. Despite some claims made at a 1991 Miami Beach information security conference, there are no upcoming new breeds of hardware viruses that cause monitors to overheat and blow up, according to experts like Martin Marietta's Peterson. Safeguards in new screens prevent that, as well as burnout.

LANs HIT HARD. Networks, of course, can facilitate the spread of viruses. Within minutes after a virus is copied to a local-area network (LAN) server, hundreds of other computers can be affected, warned a 1991 report by the U.S. National Institute of Standards and Technology (NIST), Gaithersburg, Md. Recovery takes the work of several people over several days.

Though networks are vulnerable, protective measures do exist to limit damage and keep the network running. Practitioners note that LANs with virus protection and other measures can inhibit infections. Much commercial software is now addressing LAN security so "you can make an active LAN defense," said Peterson. He noted one instance where a LAN with more than 2000 nodes was "massively infected" by a virus but kept operating and had to be shut down for cleanup only one hour in the early morning.

Wireless LANs being introduced for convenience' sake may not only facilitate eavesdropping but also virus implantation. Lieutenant Colonel Christopher Feudo of the U.S. Army, who is completing a Ph.D. dissertation on the topic, found it relatively easy for a slow hostile LAN to slip a packet of 512 bytes into a LAN expecting a message from another friendly LAN. There are scores of viruses of less than 512 bytes. Feudo added that many LAN packages now have some security features that make virus insertion more difficult, but still possible.

> If you don't report computer crimes, you pass the problem along—and one day you'll get it back

Most manufacturers to date have not pursued aggressively the development of virus-resistant systems. Several have, however, set up their own virus-monitoring systems, and at least one is even marketing an antivirus service to the public. But demand so far has not been great.

As yet, big manufacturers like IBM Corp. and Microsoft Corp., Redmond, Wash., have shown little interest in developing virus-resistant hardware or operating systems. Back in the early 1980s, when budding design shops were struggling to optimize processors for speed, no one was concerned about protection against nonexistent viruses. Now as inexpensive chips have gotten faster, adding antiviral options without slowing basic operations has become more feasible.

The manufacturers themselves, of course, are not immune to viruses. IBM set up a virus-monitoring system three years ago that monitors hundreds of thousands of machines internationally within IBM along with those of some customers. Jeff Kephart, a researcher at IBM's Thomas J. Watson Research Center, Yorkville, N.Y., noted that the prevalence of any particular virus tends to increase for a year or two and then plateau at very low levels. However, the total number of viruses has been rising at a roughly linear rate during the last two years, due to an increase in the number of different viable virus strains. The rate of IBM-tracked virus incidents per 1000 PCs per quarter tripled from 0.4 in the fourth quarter of 1990 to 1.1 in the fourth quarter of 1991.

This rise in incidents spurred IBM last fall to begin marketing its antivirus service to the public for $50 000 per initial year and $24 000 in subsequent years. This spring, however, the computer giant changed its rates. A company with 1–500 computers can get the service for $4000 a year (potentially $8 per machine); one with 1001–2000 computers pays $13 500 annually.

Included in the service are all existing and newly developed IBM software detection and cleanup tools; a toll-free bulletin board number for alerts and upgrades; a 24-hour, seven-day-a-week emergency assistance team; the offer to reverse-engineer any new virus within 72 hours; and various security-related documents. An on-site class is also available for an additional charge.

Yet "no one is demanding virus protection be put in," said Martin Marietta's Peterson, "probably because not too many know it can be built in." To some degree, manufacturers are inhibited by the desire to keep new upgrades compatible with old versions.

"Once you understand the architecture, there are only limited areas where a virus can hide," said Peterson. At his desk, he has a 16-MHz 386SX Zenith desktop with four layers of antivirus software and integrity protection. Even so, "many observers think it is a much faster machine," he said.

Although Peterson has devised a virus protection program at Martin Marietta, he declined to discuss improvements in detail for security reasons. But he claims proper implementation could immunize computers to most of today's viruses and make it "an order of magnitude more difficult to write new ones."

DETECTION MADE SIMPLE. As viruses become more sophisticated, their means of detection must be simplified. The same things

that make PCs compatible—such as the basic input/output system (BIOS), the layer under an operating system like MS-DOS or OS/2—also make it easy to detect common viruses. One means is to precede operation by using such simple techniques as a checksum, in order to verify that no BIOS code has been corrupted.

The *Virus Bulletin*'s Wilding said the growing number of virus varieties is already spurring nonvirus-specific detection techniques, "particularly the widespread adoption of cryptographic checksumming" ["Cryptography = privacy?," pp. 29–35]. Both Microsoft and Apple Computer Inc., Cupertino, Calif., recently announced new software initiatives that will include security services using such digital integrity checks.

Since software is always vulnerable to manipulation, some are exploring hardware fixes for certain applications—even though they may be more expensive than software schemes. Lance J. Hoffman, ■ GWU computer scientist, and Paul Clark, a Ph.D. student at GWU who also works at Trusted Information Systems Inc., Glenwood, Md., are developing ■ read-only smart card so that a "user can carry the operating system in his wallet, and plug it into the machine." Like other smart cards, it could authenticate users and also prevent BIOS or boot-sector viruses.

Without big improvements to computer immunity, Brunnstein and others predict, viruses generated with new techniques will be even less detectable by traditional means. Current methods of scanning signatures, for example, might be unable to identify new infections within a reasonable time.

False alarms become more likely, too. As Alan Solomon, president of S&S International, Berkhamsted, England, noted, a false alarm may take a whole day to deal with, whereas removing an actual virus often takes only minutes.

NETWORK ATTACKS. Even if many companies are dealing with infections as a usual cost of business, what if they are ■ direct target? Martin Marietta's Peterson said, "I'm not really that concerned with viruses *per se* anymore, but with directed attacks," those tailored to known vulnerabilities at a specific network.

Unlike the gradual spread of virus infections by disks transferred from person to person, in microseconds a network can be broken into by anonymous intruders from across the oceans. Network hosts are usually infiltrated in two ways: by cracking weak passwords or by exploiting trapdoors in software code (written purposefully or inadvertently).

What highlighted the insecurity of networks was an attack on a network using the Internet Protocol that began shortly after 5 p.m. eastern standard time on Nov. 2, 1988. Within several hours, the Internet worm created by Cornell University student Robert Morris Jr., son of the chief scientist for the National Security Agency's National Computer Security Center in Fort George G. Mead, Md., panicked the academic computing community.

As it swept across Internet, the self-replicating program infected 1200–6000 VAX and Sun 3 computers running certain types of Unix. Many organizations, such as Lawrence Livermore National Laboratory, Livermore, Calif., severed their Internet connections and maintained an all-night vigil.

The incident has been documented in detail and is sometimes called the Three Mile Island of computing, referring to the near-meltdown of the U.S. nuclear power plant in 1979.

In retrospect, one of the biggest surprises to outsiders was that the worm exploited well-known security flaws. Until then, "there was sort of a gentleman's agreement that you don't do that sort of stuff," said Ed DeHart, who was then ■ computing manager at Carnegie Mellon University's Software Engineering Institute in Pittsburgh. He now works for the institute's Computer Emergency Response Team (CERT), ■ group of "intrusion busters" for the Internet ["Swat teams on 24-hour call," p. 22].

Today, any gentleman's agreement is off. The Internet culture has changed from that of a trusting academic enclave into an interchange that includes millions of commercial users worldwide.

Although the CERT people, like many in industry, decline to discuss security breaches and vulnerabilities in detail, many cases (once the fixes are known) are distributed in CERT advisories. The incidents vary from intrusion schemes and system configuration errors to design holes and automated attacks. A few examples, and their advisory dates, follow:

- Some users received telephone calls or electronic mail (which can appear ■■ though from ■ site administrator or root) requesting them to run ■ "test" program, previously installed by the intruder, which prompts the user for his password. When the user executes the program, the user's name and password are e-mailed to a remote site (April 18, 1991).
- Several intrusions into Internet-connected Unisys systems were reported. "The intruder(s) gained access to these systems by logging into vendor-supplied default accounts...." Gary Garb, corporate computer security officer for Unisys Corp., Blue Bell, Pa., elaborated: the Unisys U5000 series Unix systems are delivered with ■ number of system *logins*. The *logins* are not, however, password-protected when the customer receives the system. Unless the customer secures these *logins*, the system is vulnerable to unauthorized access (May 7, 1990).
- "Automated tftp [trivial file transfer protocol] probes have attacked Internet sites throughout the world over the last few days, retrieving password files. These might later be cracked enabling *login* to accounts and possible access to the root account." The recommended solution was to disable tftp immediately if it was not needed or to reconfigure it to deny access to the root directory (Sept. 27, 1991).

Because of the steady flow of such advisories by CERT and other groups, many of the more easily exploitable vulnerabilities in, say, operating systems have already been uncovered and fixed by manufacturers. However, "some of the vulnerabilities we're studying now are very subtle things," said Steve Mick, leader of the computer incident response team at Lawrence Livermore National Laboratory. "The level of expertise needed to discover them is quite high."

Mick added that "the person who knows a little bit about Unix or VMS would not be able to do this." Even the widely publicized Dutch hacking incident of early 1991 took advantage of known simple vulnerabilities. But it took months of manual work to do.

Now CERT's DeHart is seeing some automated attacks, most rather simple, in which ■ code-cracker writes ■ program to do his dirty work automatically after he has logged off. What alarms him more is the discovery of "new vulnerabilities in different protocols that in 1988 were never even imagined."

"It only takes one or two people to discover a vulnerability," DeHart said, "but using e-mail and other means, they spread the word throughout the intruder community," often faster than users can respond. CERT does not monitor hacker bulletin boards but gets tips from people who do, he added.

> E-mail seemingly from a system administrator can fool people into divulging passwords to an intruder

SECURITY DILEMMA. The traditional difficulty for security-minded people is that systems are usually designed with legitimate operation in mind—that is, to promote speed, compatibility, and convenience. Security is often an afterthought. (Exceptions exist, like the Multics timesharing operating system, designed by the Massachusetts Institute of Technology [MIT], General Electric, and Bell Laboratories in the late 1960s. Though it became ponderous and never caught on, it did help Bell Labs' Ken Thompson create Unix.)

"The real problem is the architecture," said GWU's Hoffman. "We're using an architecture that is permissive." Chuck Cole, computer security manager at Livermore, agreed: "There'll always be new ways of exploiting the operating systems," he said.

To combat some vulnerabilities, a sizable

Some of today's computer viruses, in order of appearance

Name	Type	Size (bytes)	Damage	Prevalence	Antidote	Remarks
Stoned	Program (file), memory resident	480	Overwrites the file allocation table (FAT) on some hard disks and parts of the root directory on some disks	Including its derivatives, the most widespread type of IBM PC virus in the world	Any virus scanner that knows about it, any integrity checker that checksums the master boot record	First to infect master boot record
Jerusalem	Program (file), memory resident	1808 (plus 5-byte signature in command file)	Damages executable (EXE) file with internal overlay structure; causes multiple infection of the EXE files so they grow too large to fit in memory; slows host computer; deletes files on Friday the 13th	Including its derivatives, the second most widespread IBM PC virus in the world	Any virus scanner that knows about it, any monitoring program, any integrity checker	First to infect files in the PC world, first to reside in memory
Cascade	Program (file), memory resident	1701 or 1704 (two variants)	Characters appear to "drop" from screen and pile up at the bottom	Widespread, third most common virus in western Europe	Same as above	First to use variable encryption to hinder scanning; only short scan string is possible
Thanksgiving	Program (file) and system	1253	Overwrites the FAT on some unusual hard disks	Not widespread	Same as above	First to infect both files and master boot records (multipartite)
Icelandic	Program (file)	656	On disks larger than 10M bytes, constantly marks clusters as bad	Extinct	Any virus scanner that knows about it, any integrity checker	First to use tunneling technique to bypass monitoring programs
Yankee Doodle	Program (file)	2000–3000 or so	Plays the tune "Yankee Doodle" at 5 p.m. (some variants play when Alt-Ctrl-Del is pressed)	Relatively widespread	Same as above	First file infecter to use sophisticated tricks (stealth methods) to avoid detection; only virus to use self-correcting Hamming code to self-recover from modifications
Dark Avenger	Program (file)	1800	Overwrites random sectors on the disk with its body	Widespread	Any virus scanner that knows about it, any integrity checker (virus must not be active in memory when they are used or they will spread the virus to each file they check)	First fast infecter; infects EXE files when they are accessed for any reason
Nomenklatura	Program (file)	1024	Sometimes swaps random words of the FAT, slowly corrupting the file structure; no reliable way to determine which files are corrupted	Relatively widespread in UK	Same as above	Probably the most dangerous; originated in Bulgaria and sent by modem to the UK; spread by Trojan horse in a U.S. virus scanner; usually corrupts backup files before discovery
Starship	Program (file)	About 3000	Displays a picture of a sky full of stars and plays a tune	Relatively widespread in Commonwealth of Independent States	Any virus scanner that knows about it (checking programs must be installed on virus-free system or they will not detect virus)	Combines several modern virus technologies: stealth, multipartite, polymorphic, slow, tunneling; it uses no system memory as it resides in video RAM; infects master boot record by changing only 3 bytes in the partition table data
Dir II	System virus: directory infecter	1024	Infected programs can be destroyed if copied; under Compaq DOS 3.31, destroys the file system	Relatively widespread	Any virus scanner that knows about it; any integrity checker (virus must not be active in memory when they are used or they will be unable to detect it and spread it to every directory they check)	Completely new type that infects directories, not files; extremely fast—a few directory commands could lead to the infection of every EXE on a hard disk without noticeable delay; full stealth and advanced tunneling
Bomber	Program (file)	4096	Stops some infected self-checking programs	Recently detected in Europe	Virus scanner that can check *entire* file, monitoring program, and integrity checker	Splits into several parts and randomly distributes them in the infected file; combined with a strong polymorphic technique, could make scanning useless

Source: Vesselin Bontchev and Klaus Brunnstein, Virus Test Center, University of Hamburg, Germany, for *IEEE Spectrum*

cottage industry for information security sprang up during the 1980s. Aside from virus protection software, companies are able to buy gear to distinguish users by the way they type in their ID and passwords, and also purchase retina scanners, smart card scanners, and a host of other products ["The quest for intruder-proof computer systems," *Spectrum*, August 1989, pp. 22–26].

Robert C. Bales, director of the National Computer Security Association, which recently moved to Carlisle, Pa., said that some of these products are innovative. But "how much consumers are willing to spend is really the key. It could be easy to spend as much on security as the PC itself"—an option, he admitted, that was not too likely.

Nevertheless, some cheaper alternatives exist. A number of systemwide changes are being employed and many using cryptographic techniques and expert systems are in the works.

Many intrusions, too, are simply the result of poor implementation. Referring to recent studies of intrusions, the National Security Agency (NSA), in response to written questions from *Spectrum*, told us: "Proper application of existing technology would have prevented these penetrations or at least forced the intruder to develop and employ more sophisticated attacks."

The first line of defense is choosing passwords that resist password-guessing programs, which may use large multilingual dictionaries, names of people, rock groups, car models, and acronyms common to computer professionals. Easily obtained personal data—such as license plate numbers, social security numbers, and birth dates—should also be avoided.

CERT recommends using an easy-to-remember phrase, such as "By the Dawn's Early Light," from which one might form: "bthDeLi." The Whole Earth 'Lectronic Link (Well) manual for the San Francisco–based network urges alphanumerics of the same vein, such as "ATo2C%," which can be remembered by *A Tale of Two Cities*, plus a percentage sign. (Undoubtedly, both these examples will be added to password guessing programs soon, if they have not already been.)

Although computers can eventually crack any 7- or 8-digit password, even encrypted ones, some are "much easier to break than others," CERT's Barbara Fraser said. The point, she added, is to make the job more trouble than it is worth. As employees and contractors change, so should the passwords. Vendor-supplied default passwords should also be changed during installation of the system and whenever it is upgraded with new software.

Other general suggestions include: create guest accounts with set profiles to do limited things; use passwords that expire (rather than those that are recycled); and, as urged in a NIST report, "Don't include messages such as 'Welcome to the Payroll Accounting System' that may cause the system to be more attractive to unauthorized users."

Management backing and documented procedures are critical, too ["Raising security consciousness," below]. Buck Bloombecker, a lawyer who heads the private National Center for Computer Crime Data, Santa Cruz, Calif., which collects crime statistics, said that especially useful is a documentation of procedures along with the names of people who have permission to access the system, and at what levels. A "Hollywood hacker" case in which information was taken from the Fox TV broadcasting network computers bogged down over whether the person was still officially an employee or not; the case was consequently settled out of court.

"More and more, the people responsible for the machines are not trained system administrators, so it is more important that the product be secure out of the box," said Fraser. Although that has not yet happened, some improvements have been made within the last few years.

TRANSPARENT CHANGES. Ways of countering intrusions include password-checking systems, call-back systems, and the employment of cryptography. Sophisticated

Raising security consciousness

Increasingly concerned over computer virus infections, Martin Marietta Corp.'s Electronics, Information and Missiles Group, Orlando, Fla., convinced management to back an extensive security program in the late 1980s. In November 1991, the Computer Security Institute, San Francisco, awarded its first Computer Security Program of the Year Award to the Martin Marietta group, which has about 9000 employees. The award recognizes corporate achievement in developing and implementing an information security program. The following is an insider's view of the program. —*J.A.A.*

Computer technology is key to the wide variety of advanced weapons systems designed, developed, manufactured, and supported by Martin Marietta's group. Integrated databases are used in areas ranging from engineering and manufacturing to business systems, procurement, and product support. These greatly enhance productivity and the ability to design and deliver complex defect-free products.

The computer security program, therefore, is critical, and it does not stand alone. It is part of an overall commitment by the group to total quality management—an effort meant not only to enhance the company's competitive position in the aerospace and defense industry, but also to ensure the delivery of quality products.

In developing its computer security program, the group was guided by a threat and vulnerability analysis derived from various outside studies but tailored to internal corporate needs. Another document, the Corporate Computer Security Issues and Strategies, declared that electronic information has value and deserves commensurate protection. It adds that employees are to blame for four out of five cases of damage to, and breaches of, computer security, and are often unaware of their mistakes.

To remedy this weakness, a computer awareness program was developed and implemented in 1990 and made mandatory for all employees.

The basic-level awareness course addresses the screening, detection, and eradication of viruses; controls for limiting access; and software licensing and copyright laws. It has evolved into computer-based education, which is available on-line for all employees and in which they must take and pass refresher courses each year during their birth month.

To support this training, computer security laboratories have been set up and staffed at every location of any size. Any time an employee brings computer hardware or software into the plant, he or she is required to visit the nearest lab, which screens for viruses. Thus, only virus-free items leave the lab for use at that location. When a virus is found, the lab not only eradicates it, but also follows the audit trail so as to determine its source and to take appropriate actions within the community or within the industry.

The screening labs are supplemented by virus-response teams, whose members are specially trained and certified. A system for rapidly reporting suspected viruses to these teams has been developed on the basis of hot lines to the group's existing service desk. The system logs every call and corrective action and includes an audit trail. Employees reporting a suspected virus obtain an immediate response from the virus-busting teams, which can be contacted 24 hours a day, 365 days a year, through a network of telephones, beepers, and electronic mail.

Comprehensive documentation of policies, procedures, and directives has been made available on-line to employees to ensure they all understand the group's position and their own responsibility for computer security. Procedures in a manual called "The Protection of Electronic Information" are mandated at each company operating unit. They include designating a unit information security coordinator, conducting annual educational and training programs in electronic information protection awareness, and performing an annual threat and vulnerability analysis. Also required are system access controls, back-up and recovery processes commensurate with risk assessment, and the documentation and testing of disaster recovery plans. Yet other requirements spell out the need to implement procedures to prevent, detect, and respond to viruses; to adhere to software license agreements and copyright laws; and to preserve the security classification of information transferred to electronic form. In addition, an Information Architecture Specification has been developed that provides further technical guidance.

Because the group is committed to a three-tier computer architecture—growing utilization of personal computers, extensive networking with servers, and the use of mainframe computers—a computer hardware and software assurance program is

multilevel secure systems are being planned—both in the United States and in Europe.

"There are a lot of technological advances that can make networks more secure and at the same time have little impact on the users," said CERT's DeHart.

Password-checking programs can now assess how tough a password is to crack, and can reply, "That is a very excellent password!" Call-back systems can reduce threats to call-in systems; especially effective are those systems that only authorize certain phone numbers to be called back (such as employee's home phone). More users are also employing the Data Encryption Standard (DES) or other schemes to encrypt data files and passwords.

One of several firms coming out with secure e-mail package is Trusted Information Systems. Its privacy-enhanced mail software will be made available for use free of charge to qualified Internet users. (U.S. export constraints on cryptography limit its distribution.) Mitre Corp., Bedford, Mass., is also examining private e-mail.

Also being employed or developed are various network security packages. Nowadays, because of network vulnerabilities, an installation like the Livermore National Laboratory, which has classified data on nuclear weapons and Star Wars, maintains separate networks. Rather than any sophisticated tools, "the classified side has distinct air gap," said Livermore's Cole. There are no connections to the outside world because that would be too risky.

The NSA plans to spend several hundred million dollars through 1999 to help bridge various security levels, in what it calls "the largest current technological challenge we face," the development of multilevel secure (MLS) systems.

> No one is demanding built-in virus protection, probably because few people know of it

The NSA told *Spectrum* that these systems would "provide access control and security management across the entire information system, from individual workstations to the interconnecting wide-area networks."

Current efforts in both industry and government focus on how individual components such as operating systems, database managers, and LAN controllers can be trusted to function at appropriate levels of security. By the mid-'90s, the NSA hopes to have these components interconnected into an initial system based on MLS capability, and then expand to diverse networks.

"For national security systems, the focus of NSA's work, this could encompass the entire range from unclassified through top secret," the agency stated.

Industry may find it useful, too. The basic problem of having multiple levels of information and users with different access levels is the same, the NSA observed, and the same technology can solve the problems. "Unclassified systems may have many users, but need to restrict their access to medical, personnel, financial, and other sensitive information," the agency noted. They also need to separate authorized and unauthorized users (hackers), and isolate certain data, such as viruses.

EUROPEAN EFFORTS. In Europe, several projects are also addressing multilevel secure systems. One, called Chots, is already being deployed at the Ministry of Defence in the United Kingdom under contract of US $500 million with International Computers Ltd. (ICL), London.

Plans call for at least 18 000 terminals (and possibly 30 000 additional ones) in a Unix network distributed over 30 sites. (The system's security is rated at roughly high mid-range, or B1 level, as specified in the NSA's Trusted Computer Systems Evaluation Criteria or Orange Book guidelines.)

Some of the security in Chots may be extreme for some organizations. For instance, audible alarms go off if a terminal's panel is forcibly removed, and magnetic badges are scanned as part of the user ID. Chots also has e-mail alarms; thresholds to thwart numerous unsuccessful log-in attempts; and 32 levels of user classification (such as "secret" or "confidential").

Chots is designed to be unobtrusive to the user. With it, productivity is expected to rise 20 percent because its environment makes extensive use of e-mail, personal and group databases, business graphics, and so on. The main drag on system performance will be the auditing data, ICL engineers said, which will be compressed and may vary at different security strata (for example, keeping very extensive records at "secret" but fewer at "confidential" levels).

The European Community, through its R&D in Advanced Communications Technologies in Europe (RACE) II program, aimed at developing applied technologies, is sponsoring Project Sesame. Its goal is to create secure distributed-computing network for mixed brands of computer systems, scalable to networks as extensive as the Internet. The effort involves ICL, Siemens Nixdorf Information Systems in Germany, and Groupe Bull of France.

The first phase, writing code to demonstrate security standards of the European Computer Manufacturers' Association, is finished, said Tom Parker, an ICL fellow and chairman of its technical security strategy committee. Now the Project Sesame team is writing open-system software components to be ready for market by 1994. When completed, the software will enable user to log in just once within a large distributed network and access all data that he or she is authorized to. Currently, a user "has to remember a lot of difficult passwords" to access different levels, Parker noted.

According to him, Sesame will have some advantages over Kerberos, an MIT-developed network security system. For instance, Kerberos relies on secret-key encryption, which when scaling up to large networks means managing unwieldy numbers of keys that must be kept secret and up-to-date for each user. In addition, European countries have a hodgepodge of encryption restrictions—both across and within borders. (EC members, however, are at work to create a more uniform policy.)

One of the advantages of Sesame is its so-called privilege attribute certificate scheme. This contains user's identification, the group he is in, his role in the organization, his security clearance, his audit ID, nonrepudiation identifier, and so on. The certificate gets sent along to every application or level the user wants to use. Keeping the record with the individual makes for easier management, Parker said. For instance, if

being implemented for all computer systems at all the Martin Marietta group's locations. The program builds on employee awareness education and includes hardware and software to provide virus protection and also self-audit capabilities.

In parallel, software libraries and other improvements are being implemented to better manage the entire evolving configuration of hardware, software, and communications.

Along with the security efforts, tests of host computer disaster recovery are conducted twice a year. The tests address all aspects of communications and critical applications in particular. Preparations are under way to include the group's distributed systems as well as its mainframe-based systems.

In sum, computer security is not a one-shot deal. Rather, its adequacy must be kept under constant review because of the rapidly changing technical environment. Comprehensive solutions to computer security problems in effect underwrite the Electronics, Information and Missiles Group's growing investment in, and reliance on, computer technology and thus preserve a critical lifeline to the group's continued health and prosperity.

—John M. Castle and John Uffelman

John M. Castle is a former manager, management systems, special initiatives, for Martin Marietta Corp.'s Electronics, Information and Missiles Group, and John (Bud) Uffelman is a manager, information systems, data security, for the group. A. Padgett Peterson of the company's technical computer center also contributed to this feature.

a manager goes on vacation, she can authorize her subordinate to use her access privileges while ensuring that the subordinate keeps his audit identity.

Like some other secure schemes such as one by Digital Equipment Corp., Maynard, Mass., Sesame is to use a mix of public- and secret-key cryptography. Public-key systems are better for scaling to large systems; secret-key ones are more efficient for encryption within a special domain of a large network. To ensure the integrity of messages, Parker said Sesame is looking favorably at the U.S. government's proposed Digital Signature Standard ["Cryptography = privacy?," p. 29–35].

Sesame is to have a basic E-3 level of security (a medium level as measured by Europe's Information Technology Security Evaluation Criteria). This is sufficient for many commercial operations, Parker said, without posing undue costs and maintainance difficulties. At present, authentication is based simply on passwords, but the protocols are designed to permit smart cards and other identifiers to be added.

ICL is working with Hughes STX to commercialize the results of Chots and Project Sesame. With a flexible menu of attributes, the companies claim they will offer the first open systems secure network for commercial markets.

VIGILANT GUARDS. Another area to which industry and government are turning for help to stem intrusions and fraud is expert or knowledge-based systems. A couple of advanced expert systems, already in prototype, could be scalable to thousands of network users.

Financial companies are using several expert systems. American Express Co., New York City, uses one to authorize purchases based on previous habits, locale, time, and so on. Wells Fargo Bank and Bank of America, both in San Francisco, recently began using one for new accounts data authentication, according to Donald Parrott, an assistant vice president for Bank of America.

Bank of America processes 10 000 new accounts daily and had seen a 20 percent rise in "sundry losses" due to fraud from 1989 to 1990. Now an expert system can flag criminals on the basis of excessive account activity, access abuse, automated teller machine abuse, the falsifying of new accounts, and the opening of multiple accounts.

SRI International, Menlo Park, Calif., is creating the Intrusion Detection Expert System (IDES), which monitors about 50 aspects of user behavior (such as what files they access, what times of day and week, and so on) to compile a statistical profile for each *login*/password account. In addition, the system knows the network's likely vulnerabilities and intruder habits. With this mix, IDES, it is hoped, will thwart both outside crackers and authorized users who rove in unauthorized accounts.

Dormant viruses and worms are also targets, according to Teresa Lunt, SRI's director of secure systems. IDES will detect and record misdeeds almost immediately and will be on guard 24 hours a day.

The system, whose chief sponsor is the U.S. Navy, runs on a separate Unix-based workstation; it should be mostly transparent to users, although there is some overhead penalty because each machine's operating system collects audit data on its users to send to IDES. The existing IDES prototype is hooked to about a dozen workstations at SRI, but if developed, it could be scalable to hundreds and possibly thousands of network users, said Lunt.

> A lot of technological advances can make networks more secure without having much impact on the user

The U.S. Federal Bureau of Investigation (FBI), Washington, D.C., has been so impressed with IDES that it is testing its use in protecting an IBM mainframe system. (The FBI declined to comment on its expert systems projects.)

If privacy and legal issues are satisfied, IDES may find applications with various networks and perhaps automatic bank tellers. An as-yet-unresolved technical weakness of IDES is that a habitual miscreant will go undetected since IDES will see his behavior as normal.

The Livermore National Laboratory, which has more than 12 000 computers in its unclassified network, has just begun using its prototype distributed intrusion detection system (DIDS), a multimillion dollar project funded mainly by the U.S. Air Force. It is distinguished from most research in the area in that it monitors all traffic between network computers, not just the activity of one host computer.

An analogy would be the ability to monitor the doors of all the buildings in a city block, said Doug Mansur, leader of the DIDS research team. Each door knob rattle reveals little on its own, but a pattern of successive rattles may sketch an intrusion attempt. Once an intrusion is detected, the system preserves information about the attempt to assess the type of attack, the extent of damage, and how to counter the threat. The data may also help locate the attacker and serve as evidence for prosecution, added Livermore's Cole.

U.S. GOVERNMENT MOVES. Computer crime fighting is being given a higher priority by the U.S. government. Already in the works are plans to develop a technology standard setting up security criteria for all Federal agencies. And industry groups, too, are pushing for stronger security measures by endorsing system principles that are accepted internationally.

Under a Memorandum of Understanding between NSA and NIST, the two agencies have been exchanging work plans for the past three years regarding "research and development affecting systems processing of unclassified information." The pact calls for the two to work on a Federal Trust Technology Standard that will provide computer security criteria for the entire U.S. government, and, by extension, private industry.

The agencies are also shoring up security across Federal agencies, based on National Security Directive 42 of July 5, 1990. And an independent nonprofit International Information Security Foundation (I²SF), based on a recommendation of a 1991 National Research Council report, "Computers At Risk," is forming at SRI International.

Three U.S.-based industry groups—the Information Technology Association of America, the Computer and Business Equipment Manufacturers Association, and the Information Systems Security Association—recently endorsed the need for a smaller foundation, aimed at facilitating the adoption of system security principles that are generally accepted internationally. The belief is that a basic level of protection should be expected, without having to consult information security specialists. Chris Castro, executive director of I²SF, said such security principles regarding hardware would be the foundation's first project.

The FBI and its parent organization, the U.S. Department of Justice, are restructuring this year to give computer crime fighting a higher priority. Included are more training for the 10 000 FBI agents, examination of viruses and network intrusions, and the creation of a Computer Analysis Response Team, analogous to other FBI forensic labs like fingerprinting. Last April in Charleston, S.C., the FBI sponsored its first international computer crime conference, which was attended by law enforcement officials from Europe, Australia, and Canada.

"We need to have a cooperative spirit between users, industry, and government," James C. Settle, an FBI computer crime specialist, said. Law enforcement can be only part of the deterrent, he emphasized. Industry must take precautions.

Like many others, Settle believes only a small percentage of electronic crimes are reported, and urged more organizations to go public with them. While victims can report crimes anonymously to the FBI, they must commit to go public in order to get search warrants, Settle noted. "If you don't report crimes," he said, "what you do is pass the problem along and one of these days you'll get it back." ◆

Cryptography = privacy?

Cryptography is becoming a powerful tool for information security, but U.S government restrictions on its use or export still apply

Rarely in the arcane world of cryptography and electronic spying does a decision stir so much controversy. The ruckus is over a proposed standard for electronically authenticating messages. But the wider dispute extends to all of modern cryptography, whose techniques not only enable electronic commerce but are crucial to protecting information in computers and in transit.

The proposal for the so-called U.S. digital signature standard was evaluated by scientists at the U.S. National Institute of Standards and Technology (NIST), Gaithersburg, Md. Up until December 1990, they recommended a code-making method known as RSA for adoption as a U.S. government standard, *IEEE Spectrum* has learned. RSA was already the method preferred by industry, and royalty payments by the U.S. government would be waived.

But a change of mind occurred. Nine months later, on Aug. 30, 1991, NIST hastily put forth an entirely new algorithm for public review. Called the Digital Signature Standard (DSS), it was developed by the U.S. National Security Agency (NSA), Fort George G. Meade, Md. Its basis is the public-key technique of discrete logarithms published by Taher ElGamal in 1985.

Many in industry were, to put it mildly, disappointed by the news. The NSA not only makes codes but, more importantly, breaks them to intercept intelligence from international telecommunications traffic. This dual role seems suspect to some people: if codes influenced by NSA are crackable, the agency's intelligence mission becomes easier.

In short, speculation is rife over whether the powerful NSA violated the 1987 Computer Security Act by unduly pressuring NIST during those few months last year. The Washington, D.C., office of Computer Professionals for Social Responsibility took the U.S. government to court to comply with a Freedom of Information Act request regarding the institute's motivation in proposing the standard. NSA and NIST are resisting for the most part, saying that the way decisions are made is an internal matter. Lynn McNulty, a NIST associate director, has said "NIST made the final choice" on the basis of technical assistance from NSA and others.

In a statement to *Spectrum*, NSA denied giving NIST "any opinion on the use of RSA as a standard for encryption" but said it was "inappropriate to discuss" its role in the mysterious dropping of RSA as a standard for digital signatures. The NSA said that "NIST came to NSA requesting technical assistance." [See "The NSA speaks . . ," p. 32.]

Spectrum has learned from U.S government sources requesting anonymity that the RSA technique, patented by the Massachusetts Institute of Technology, Cambridge, had been readied by NIST as the standard for several months and was dropped in December 1989 with no alternative in sight. Not until early spring of 1991 did NSA present the algorithm of choice to NIST. Even on background, sources declined to detail reasons behind the decision, although one mentioned that legitimate national security factors had come into play.

> The U.S. government won't say why it prefers the National Security Agency's encoding scheme

What actually happened is of more than academic interest, for it could have a big impact on the information age. During the 1970s, when the U.S. government openly developed its first cryptographic algorithm (the Data Encryption Standard), the Defense Department's NSA oversaw information security for both classified and unclassified information. The 1987 Computer Security Act transferred the unclassified role to the Commerce Department's NIST. Whether Commerce's NIST can assert itself more in the post-Cold War era may affect not only the standards but the export of encryption products.

POSSIBLE PANACEA. Cryptography itself is seen as the only effective means of ensuring security and privacy in communications and within computers. For example, the Software Publishers Association, Washington, D.C., has estimated that within five years most mass-market software programs will include data, text, and file encryption capabilities.

"Our customers have told us," said Nathan P. Myhrvold, vice president of advanced technology and business development, Microsoft Corp., Redmond, Wash., "that without this security they will be much more hesitant to move critical information from mainframes and minicomputers to desktop PCs."

One way to immunize computers against present and future viruses is for manufacturers to attach digital signatures to their software. This acts as a tamper-detection seal and allows users, each time they run software, to determine its integrity beforehand.

The telecommunications realm, of course, is also affected. The trend is for engineers and corporate officers to exchange proprietary information not within private boardrooms or secure buildings but through networks. "Encrypted store-and-forward data, video, facsimile, and certified electronic mail will soon be as common as locked filing cabinets," said Kenneth G. Ingram, AT&T director of product development.

Besides wrapping electronic information in secrecy, modern cryptographic techniques can also all but guarantee authenticity, ensuring that a message came from John Doe and was not a forgery and that the digital stream's integrity is unimpeachable. Additional applications, current or imminent, include more electronic commerce using smart cards, secure portable computers and wireless networks, and authenticated access to thwart intruders and protect data bases.

Yet adoption of these commercial uses of cryptography is being hindered by government restrictions, a situation perhaps epitomized by the DSS proposal. Stephen T. Walker, president of Trusted Information Systems Inc., a small information security

John A. Adam Senior Associate Editor

0018-9235/92/$3.00©1992 IEEE

R&D and consulting firm in Glenwood, Md., worked for 22 years at the Department of Defense, including the NSA. He called the NIST/NSA signature algorithm "an unfortunate proposal that gives the impression that the Government is trying to solve the problem while it is merely hiding the real issue for several more years."

The Computer System Security and Privacy Advisory Board, established by the U.S. Congress, reacted similarly. It unanimously called for a national debate on the widespread use of cryptography, to conclude by June 1993; most board members, including Walker, said any decision on the proposed DSS should await the national debate.

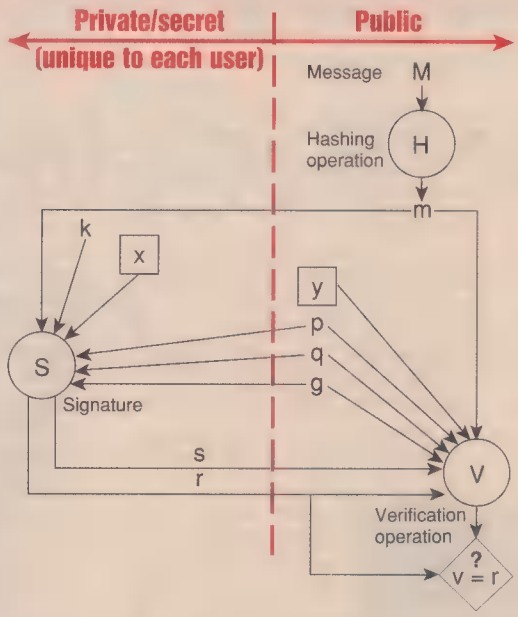
Many of the issues may seem as convoluted as the encryption techniques. But central to understanding them is an acquaintance with public-key cryptography (PKC).

KEYS FOR PUBLIC. Throughout much of history, spies, diplomats, and the military have been using the same basic principle for their code work. For instance, Julius Caesar apparently used a simple substitution algorithm, so that VENI VIDI VICI could be transformed into YHQL YLGL YLFL. To ungarble the message, the enciphering scheme is merely reversed, and each letter is moved three places to the left in the alphabet. It is a symmetrical process whose security depends on keeping the algorithm (a cyclic substitution of the alphabet) and the encryption/decryption key (the value of three) secret. Also essential was the ability to change keys (any value from 1 to 25) and to let only authorized parties know.

In the two millennia since, many improvements have enhanced Caesar's scheme of using secret keys (especially with the development of machines), but the basic principle remained the same until November 1976. That is when Whitfield Diffie and Martin Hellman, two young researchers at Stanford University in California, published their paper "New Directions in Cryptography" in the *IEEE Transactions on Information Theory*. It put forth a revolutionary kind of asymmetric, public-key cryptography. PKC, rather than employing the same key formula to encrypt and decrypt data, uses a corresponding pair of keys. One key encrypts; another key decrypts. Because of this asymmetry, only one of the keys need be kept secret; the other may be freely distributed because it is computationally impractical to derive the private key from the public one. What's more, either of the keys can be used for encryption.

The implications of this private-public combination were far-reaching. Cryptography became applicable to many commercial transactions, such as authenticated electronic banking, private electronic mail, and internetwork commerce, and many other clever applications. PKC enabled or influenced the three major realms of contemporary cryptography—electronically signed-and-sealed data known as digital signatures; the practical digital distribution of crypto keys;

The proposal for a U.S. standard for digital signature encoding



The U.S. government is proposing that a new cryptographic algorithm become a standard to electronically verify the integrity and source of unclassified information. Known as the Digital Signature Standard (DSS), it works somewhat like a letter sealed in a transparent envelope. By checking the signature on the letter and the seal on the envelope, any receiver can verify the intact state of the message and the identity of the sender. The actual text is readable by anyone along the route (so international restrictions on encryption need not apply).

One aim of the DSS is to make paperless transactions initiated by the Government easier. Like other so-called public-key signature techniques, the DSS is meant for any use that requires integrity assurance and identity authentication.

In using the DSS, each message sender possesses a private key for which there is a corresponding public key. The public key is assumed to be known to all members of a group of users. The private key is kept secret by its creator, enabling a unique signature to be made that can be verified by anyone with the matching public key.

The principle of cryptography is not much different from that of a combination lock, but the mathematics of cryptography is computationally complex. Long strings of numbers are chosen so that computers cannot crack the "cryptographic lock" for years to come.

For example, the 512-bit prime number, *p*, in its hexadecimal form (where a hex digit represents a 4-bit string so that "A" would be represented as "1010") might look like: D0451FFE 2C64C4ED 6B06AE36 5B7FEF9 15425E40 A37CA5F8 39865E2C FB4169A0 D825C913 0F8864FF FCF3BFBE B0273660 67AA27E2 7BFCAF40 00000000 00000001. The DSS may also accommodate prime numbers twice this length.

This is how it works when Bob in one bank wants to send a message that reads "Transfer $10 000 to GE." to Sally in another bank:

1. Bob starts with a *p* (a large prime number of 512 to 1024 bits in increments of 64 bits), a *q* (a prime divisor of *p*–1), and a *g* (a modulo function of *p* and *q*). These system parameters must already be known to Sally or can be sent to her along with the message.
2. Bob makes his private key, *x*, by simply generating a random 160-bit number. Then Bob's public key, *y*, is computed using *g*, *x*, and *p*. The public key has the same length as *p*, that is, from 512 to 1024 bits. The security of the DSS hinges on the fact that it is computationally difficult to compute *x* knowing *y*, even though it is computationally easy to compute *y* knowing *x*.
3. Bob, through some certification authority, publishes his public key. Sally is one of the recipients. He keeps his private key secret—even from the certification authority.
4. Before Bob sends Sally the message, the ASCII version of "Transfer $10 000 to GE." is run through a newly developed secure hash algorithm (proposed, as is the DSS, by the U.S. National Institute of Standards and Technology, Gaithersburg, Md.). The result is a 160-bit checksum that is devised so that virtually any change in the message (like "$100 000" or "GM") would change the checksum. It is called *m*.
5. Bob generates a secret random number, *k*, also 160 bits. The secret *k* is used with *p*, *q*, and *g* to generate a message-unique parameter of 160 bits in length called *r*. It is independent of the contents of the message (allowing it to be precomputed) and is used for comparison during verification of the message.
6. Bob then uses the results of the prior two steps (*m*, *k*, and *r*) in addition to *x* and *q* to compute a message-specific signature. The result is the signature value of 160 bits called *s*.
7. Bob then sends the actual message—"Transfer $10 000 to GE."—to Sally along with the signature—a 320-bit stub composed of *r* and *s* (each 160 bits long) concatenated. The operation can be done in under half a second on a 25-MHz 386 processor.
8. Sally receives a message, M, and the signature components, *r* and *s*. M itself is put through the secure hash algorithm. Sally computes a verification value, *v*, using Bob's public key, *y*, the signature component, *s*, the two moduli, *p* and *q*, the exponent base, *g*, and the result of Sally's hashing operation on M.
9. If Sally's computed *v* on the received message is equal to *r* (what Bob sent her as half of the signature), then Sally can be assured that Bob sent the message and that the message has not been altered. If *v* does not equal the value of *r* that she received, the message is invalid. Whether the message was modified, forged by an imposter, or just incorrectly signed cannot be determined by the DSS. If the signature does not verify, a negative acknowledgment is sent to Bob and the process is restarted.

—*J.A.A.*

CONSULTANT: Dennis K. Branstad, Computer Science Fellow, U.S. National Institute of Standards and Technology

and the traditional task of ensuring information secrecy.

DIGITAL SIGNATURES. Using the private key for encryption means that an author can uniquely "seal" information with his or her own signature. It can be sent to anyone with the corresponding public key. Authentication using digital signatures not only assures the receiver that electronic data was indeed sent by, say, Acme Bank, but also that the bank's message ("Transfer $2 million from account *y* to account *z*") has not been manipulated. [See "The proposal for a U.S. standard for digital signature encoding," at left.]

The digital signature is a code, or large number, that is unique for each message and to each message originator. A cryptographic signature specific to the originator assures the recipient of the sender's identity. Processing the message with a hash function results in a small digest dependent on each bit of information in the message.

To illustrate, assume a message in a digital string of 0s and 1s is processed in blocks of 64 bits. As the first block arrives, it is held in memory. As the second one arrives, each element in the first block is matched with a corresponding element in the second data block. If two elements are alike, a 0 is recorded; if different, a 1. This produces a new 64-bit number, which replaces the first 64-bit block in memory. The function continues hashing through the entire data stream, generating new 64-bit blocks, that are dependent on everything processed previously. The end result is a 64-bit digest incorporating information about each bit of data in the whole stream. In other words, to alter the message, even by one bit, would alter the 64-bit digest. Moreover, it should be essentially impossible to forge a message that would result in the same digest.

This digest (which authenticates the message) can then be encrypted by the user using a key unique to him or her, producing the electronic signature that can be deciphered by anyone with a copy of the corresponding public key.

The whole operation prevents forgeries but allows the message to be read openly by anyone who receives—or intercepts—it. For that reason, techniques devoted solely to digital authentication are easier to export for international use, because they do not thwart national intelligence monitoring.

DISTRIBUTING KEYS. Even the sturdiest lock is no good if its key is accessible. The same applies to cryptography. Distributing the keys securely between many users thousands of kilometers apart has been a long-standing burden.

Couriers have been the usual means. But they are slow and expensive, and hold the integrity of the entire crypto system in their hands.

Public telephone networks, however, can safely transmit keys using PKC. Security is strengthened, since new keys can be changed more easily (in fact for each message). Better yet, immediate secure communication may occur among parties with no previous relationship.

A common approach, soon to be employed on the giant Internet, is to use a PKC algorithm such as RSA to electronically transfer the keys for a secret-key algorithm, such as the Data Encryption Standard (DES). (Secret-key cryptography is still used because of its speed in encrypting long messages.)

As an example, consider two people, Joe and Mary, who wish to establish a DES secret-key communications channel. Because two DES users must both employ a single secret key, the key cannot merely be sent over the wire. It must be encrypted using the matched private-public keys of PKC, thus:

- Joe posts his public PKC key on, say, an electronic bulletin board, so it is obtainable by Mary.
- Mary uses Joe's public key to encrypt a random DES key she has created. She transmits this to Joe.
- Joe decrypts Mary's message using his private PKC key. Joe alone can decrypt the message because he alone holds the corresponding private key. (In PKC, only a matched pair of private and public keys can encrypt and decrypt.)
- Now that Joe has Mary's DES key, the fast, secure communications link can start. Any eavesdropper would only have a public key, an encrypted DES key, and a garble of Joe and Mary's DES-encrypted communications.

> U.S. officials licensing mass-market software for export treat encryption programs as they do munitions

The one pitfall here is that someone else could masquerade as Joe or Mary. This can be overcome by using digital signatures. Some certification authority notarizes Joe and Mary's public keys and this can be further checked by examining "hot lists" of compromised keys (as with credit cards).

ENCRYPTION. There would be little controversy and few international restrictions if cryptography were restricted to digital signatures such as the DSS and key exchanges. Because encryption can make communications indecipherable to anyone without a key, governments restrict its use, citing reasons of national security. It would make electronic snooping too difficult and perhaps even impossible.

The two most popular unclassified encryption techniques are the RSA algorithm for public-key cryptography and the DES for secret-key cryptography.

The RSA technique was devised and patented in 1978 by its three namesakes at the Massachusetts Institute of Technology: Ronald Rivest, Adi Shamir, and Leonard Adelman. In 1982, they formed RSA Data Security Inc., Redwood City, Calif., to license their invention and devise proprietary packages for sale.

The security of the RSA algorithm depends on the difficulty of hitting upon two large prime numbers when given only their product: in other words, factoring a large number is far harder than verifying that two or more numbers are prime factors of the same large number.

Most commercial RSA systems use 512-bit keys. Recent advances in parallel computing are making the factoring of numbers of up to 116 digits (roughly 385 bits) practical. But different modulus sizes in RSA permit keys of any size to be used, giving more credibility to its security for some time to come. Since the origin of PKC in 1976, many proposed public-key techniques have been cracked within a few years (including a few involving Stanford's Hellman, one of the conceivers of PKC). The fact that RSA has not been knowingly compromised after more than a dozen years enhances its credibility.

TRADITIONAL SECRET KEY. Public keys, which currently require extensive calculations involving large numbers, are inefficient at encrypting long messages. Secret-key encryption techniques, such as DES, are computationally much more efficient and remain the favorite for bulk encryption.

DES is the encryption scheme most widely used by international industry and the U.S. government. It was also the first cryptographic algorithm openly developed by the U.S. government. IBM Corp. responded to a Government call for proposals and in 1975 put forth the algorithm, in which a single 56-bit "secret" key is used to encrypt and decrypt. The NSA, with some of the world's best code-breakers, evaluated DES favorably but recommended redesigning some fundamental components, known as substitution boxes.

The NSA endorsement led the way to DES's adoption in 1977 as a Federal standard, but many researchers believed that NSA's influence on the substitution box design and the length of the key introduced a trapdoor that allowed the NSA to read any message encrypted using the DES. (The substitution boxes provide nonlinear complexity, transforming 6 bits of input data into 4 bits of output.)

"Unfortunately, as with all cryptosystems, there is no way of knowing if the NSA or any other organization has succeeded in breaking the DES," said a 1991 report by the National Research Council, Washington, D.C. No compromise of DES has ever

been made public. But most believe that DES has furnished sufficient encryption protection, apparently on the grounds that it is used extensively. DES can be implemented to be very fast, encrypting data at more than 100 million bits per second. It has been reaffirmed twice ▪ standard after public comments and is up for renewal in January.

Responding to ▪ *Spectrum* query on DES, the NSA stated: "We do not promote 'weak cryptography' for use by industry. . .The DES is the most common technique currently used for the Federal government information privacy needs." "We are unaware of any 'vulnerabilities' in DES when properly implemented and used for the purposes for which it was designed; i.e., for the protection of unclassified, sensitive government information. However, we do note that increased use by the U.S. Government of DES equipment makes it increasingly attractive as a potential target for adversaries.

"All cryptography has ▪ natural life span, and advances in technology will reduce the security provided by DES in the future. Because of this, we do not recommend DES for classified applications. NSA stopped certifying DES products in 1988 due to these reasons and due to the Computer Security Act of 1987 that eliminated NSA's information security role in protecting unclassified data in the government and private sectors."

DSS STRENGTHS. The U.S. government is entering the cryptographic standards arena for the second time with its DSS proposal. Using not encryption but a one-way cipher scheme, the DSS computes and verifies ▪ short code, which is appended to the bulk data (which itself may be encrypted using the complementary U.S. standard, DES).

NIST and NSA have some sound reasons for endorsing the DSS, and in response to public comments have taken steps to increase its security. In addition, the DSS offers optimum signature generation, and if approved ▪ standard, would have the Government as a customer.

The proposed DSS was defended on May 7 to Congress by NIST director John Lyons, who cited some of the factors considered in devising it. He listed the level of security, the applicability of patents, the ease of export for the United States, the efficiency in a number of Government and commercial applications, and the impact on national security and law enforcement.

A number of existing techniques were reviewed and "deemed adequate to provide appropriate protection," Lyons said in the same statement. But most emphasis was placed on appropriate security and on nonpayment of royalties by U.S. interests. (Though the U.S. government has applied for a DSS patent, it plans to issue licenses on ▪ nonexclusive, royalty-free basis.)

Unlike IBM, which gave up its patent claims to DES, RSA Data Systems maintains ▪ proprietary approach, often seeing that other groups pay to license and use the RSA technique. The RSA patent does not expire until 2000.

As first proposed, the security of the

The debate over the U.S. digital signature standard

The NSA speaks. . .

The U.S. National Security Agency at Fort George G. Meade, Md., is probably the biggest U.S. intelligence agency. While it does not talk too much publicly, even during rare Congressional testimony, the agency has responded in some detail to some questions by IEEE Spectrum *regarding its role in information security and, more especially, the controversial proposal for "sealing" electronic messages.*

"It's the definitive answer from the agency," said NSA spokesman Jerry Volker in early June. (Later in the month, much of the same information was requested by The Houston Chronicle *and was published on the Internet.)*

Part of the U.S. Department of Defense, the agency is the world's premier electronic eavesdropper. In addition to breaking codes, it makes them, developing cryptographic protection for classified U.S. telecommunications and information systems.

The NSA also influences what private industry uses to encrypt or authenticate digital information, both by developing cryptological tools and by its decisions regarding encryption equipment exports. The proposed Digital Signature Standard (DSS) is only the latest in a series of clashes between NSA and the private community. Some private cryptographers and industry believe the DSS is not needed when the Rivest-Shamir-Adelman (RSA) algorithm is already the de facto *international encryption standard.*

The intelligence agency response comes from top technical and policy persons in several NSA divisions. Their submissions were collated, rewritten, and then submitted for final approval before release to Spectrum. *Three are published below in their entirety. (Others appear, edited, in other parts of this special report.)*

Spectrum *corroborated relevant information with National Institute of Standards and Technology (NIST) officials, one of whom said, "Basically, it's correct." But the NSA does not mention that, in December 1990 after evaluating a number of algorithms, NIST was ready to recommend RSA for U.S. government use and endorsement. NIST subsequently changed its position and proposed the DSS in August 1991.*

Spectrum *also sought comments on selected NSA responses from Ronald L. Rivest (the R in the RSA algorithm) and D. James Bidzos. Rivest is professor of computer science at the Massachusetts Institute of Technology in Cambridge and a director of the International Association for Cryptologic Research in Palo Alto, Calif. Bidzos is president of RSA Data Security Inc,. Redwood City, Calif., which supplies public-key security products and licenses to companies such as IBM, GE, and Motorola. Their comments follow the NSA remarks.* —*J.A.A.*

SPECTRUM: Has the National Security Agency (NSA) ever advised the National Institute of Standards and Technology (NIST) to endorse or not to endorse the RSA algorithm [the *de facto* international standard] as a standard for encryption and/or digital signatures? Please elaborate. What is the NSA position on the RSA algorithm?

NATIONAL SECURITY AGENCY: NIST has never approached us nor asked our opinion on the use of RSA as a standard for encryption. Neither have we given them any opinion on the use of RSA as a standard for encryption.

In the process of developing a digital signature for U.S. government use, NIST and NSA examined various publicly known algorithms and their variants, including RSA. A number of techniques were deemed to provide appropriate protection for Federal systems. The one selected by NIST as the draft Digital Signature Standard (DSS) was determined to be the most suitable. We consider it inappropriate to discuss which candidate algorithms or their variants were proposed or endorsed or not endorsed by which agency during the evaluation and selection process which led to the DSS publication.

NSA's position on RSA does not differ from our position on any cryptographic technique. We have always been in favor of the use of information security technologies by U.S. businesses to protect their proprietary information, and when we had an information security role with private industry (prior to the Computer Security Act of 1987), we actively advocated use of such technologies. As far as use for Federal systems, NSA has a long-standing policy not to comment on the strengths or weaknesses of any cryptologic technique. Such comments could reveal information that might undermine the security upon which sensitive Federal operations depend.

SPECTRUM: Regarding development of DSS, how was the NSA/NIST collaboration initiated? Please clarify the trapdoor issue. (For instance, if NSA developers allowed the vulnerability of the trapdoor in DSS by mistake, what does this say about the trustworthiness of NSA equipment for classified information?)

NSA: Under the Computer Security Act of 1987, NIST is to draw upon the computer systems technical security guidelines of NSA where appropriate and to coordinate closely with other agencies, including NSA, to assure:

- Maximum use of all existing and planned programs, materials, and

DSS's 512-bit key length was questioned. In response, NIST and NSA increased the maximum key size to 1024 bits, so that users may scale up from 512 bits in increments of 64 bits, though the boost in security comes at the expense of speed.

"Trapdoor" allegations were made against the DSS. To counter them, NIST intends to specify a process by which each user can generate good prime numbers. NIST has put forward several proposals for the prime generation technique, some of which it received from the NSA. NIST's Computer Science Fellow Dennis K. Branstad, a former NSA cryptographer himself, said in June, "When all is said and done, I think we'll go with what we've suggested." Details will be in the revised DSS proposal due out later this month.

To resolve another point of contention, NIST and six other Government agencies began a study in July of infrastructure issues such as a certification authority and legal and policy issues. It is expected to take about a year, said McNulty, associate director of NIST's Computer Systems Laboratory, Gaithersburg, Md. McNulty said the revised DSS, after public comment, should be ready to be instituted as a U.S. government standard around March 1993.

Asked why these issues were not dealt with earlier, in the two years that NIST had to evaluate existing signature techniques and new ones, Branstad said: "We felt we were under Congressional pressure to get something out fast. We probably put it out sooner than we should have."

Although it is slower than RSA at verifying signatures, DSS optimizes signature generation, an advantage if computing capability is limited. For instance, a NIST prototype smart card using DSS can sign in 0.05 second (if it uses a precomputation taking 7 seconds), according to Stuart W. Katzke, NIST's computer security division chief. Verification takes 30 seconds. An RSA implementation on the same card signs in about 28 seconds and verifies in 2.5 seconds.

If DSS is approved, it may be widely implemented because of the U.S. government's push to have corporate and personal tax returns filed electronically and to make electronic payments to contractors and social security recipients.

DSS WEAKNESSES. A big technical limitation of the DSS so far is its inability to electronically distribute keys, because it cannot encrypt like RSA. In terms of economics, industry is deploring the possible expensive coexistence of two standards: RSA and DSS. Adding to industry's opposition is uncertainty over NIST's intent in promoting DSS.

The technical limitation is a policy advantage to the U.S. government. NIST's Branstad said: "For patent and export reasons, DSS was preferred over RSA. DSS as specified can't be used for encryption," so that it avoids the burdensome State Department controls on most encryption software (they are noted in the munitions control list of the International Traffic in Arms Regulations). Some have said DSS might be modified to

reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

• That standards developed by NIST are consistent and compatible with standards and procedures developed for the protection of classified systems.

Based on a subsequent Memorandum of Understanding between NSA and NIST, NSA's role is to be responsive to NIST's requests for assistance in developing, evaluating, or researching cryptographic algorithms and techniques. Early in the process of developing a digital signature standard, NIST came to NSA requesting technical assistance. As part of that assistance, NSA developed, evaluated, and provided candidate algorithms following NIST guidance.

Regarding the alleged "trapdoor" in the DSS, we find the term "trapdoor" somewhat misleading since it implies that the messages sent by the DSS are encrypted and with access via a "trapdoor," one could somehow "decrypt (read)" the message without the sender's knowledge. The DSS does not encrypt any data. The real issue is whether the DSS is susceptible to someone forging a signature and therefore discrediting the entire system. The chances of anyone—including NSA—forging a signature with the DSS when it is properly used and implemented is infinitesimally small.

Furthermore, the alleged "trapdoor" vulnerability is true for ANY public-key–based authentication system, including RSA. To imply somehow that this only affects the DSS is very misleading. The real issue is one of implementation and how one goes about selecting prime numbers. We call your attention to a recent Eurocrypt conference, which had a panel discussion on the issue of trapdoors in the DSS. Included on the panel was one of the Bellcore researchers who initially raised the "trapdoor" allegation. Our understanding is that the panel—including the person from Bellcore—concluded that the alleged "trapdoor" was not an issue for the DSS. In addition, the general consensus appeared to be that the "trapdoor" issue was trivial and had been overblown in the press.

However, at the request of NIST, and in response to the "trapdoor" allegation, we have designed a prime [number] generation process which will ensure that one can avoid selection of the relatively few weak primes which could lead to weakness in using the DSS. Additionally, NIST intends to allow for larger modulus sizes (up to 1024 [bits]) that effectively negate the need to use the prime generation process to avoid weak primes. Another important point often overlooked with the DSS is that the primes are PUBLIC and therefore can be subject to public examination. Not all public-key systems provide for this same type of examination.

The integrity of any information security system requires attention to proper implementation. With the myriad of vulnerabilities possible given the differences among users, NSA has traditionally insisted on centralized trusted centers as a way to minimize risk to the system. While we have designed technical modifications to the DSS to meet NIST's requests for a more decentralized approach, we still would emphasize that portion of the Federal Register notice [of Aug. 30, 1991] for the DSS, which states: "While it is the intent of this standard to specify general security requirements for generating digital signatures, conformance to this standard does not assure that a particular implementation is secure. The responsible authority in each agency or department shall assure that an overall implementation provides an acceptable level of security." NIST will be working with government users to ensure appropriate implementations.

Finally, we have read all the arguments [alleging] insecurities with the DSS and we remain unconvinced of their validity. The DSS has been subject to intense evaluation within NSA, which led to its being endorsed by our Director of Information Systems Security for use in signing unclassified data processed in certain intelligence systems and in selected classified systems. We believe that this approval speaks to the lack of any credible "attack" on the integrity provided by the DSS, given proper use and implementation.

Based on the technical and security requirements of the U.S. Government for digital signatures, we believe the DSS is the best choice. In fact, the DSS is being used in the Defense Message System to assure the authenticity of electronic messages of vital command and control information. This demonstration includes participation from the Joint Chiefs of Staff, the military services, and defense agencies and is being done in cooperation with NIST.

SPECTRUM: As you know, many in U.S. industry say U.S. export laws discourage or prevent U.S. firms' manufacture and use of top encryption equipment. Competitors in Japan and Europe are not as constrained. In NSA's view, what constraints should U.S. businesses be under regarding the development and marketing and the usage of the latest encryption hardware and software? Please explain. What are the tradeoffs between military and economic security?

NSA: We do not agree with the allegation that U.S. export laws prevent U.S. firms' manufacture and use of "top" encryption equipment. We are unaware of any case where a U.S. firm has been prevented

do encryption; but Branstad said that was impractical, although NIST has not fully investigated the possibility. Unlike the DSS, RSA is a full-fledged crypto-algorithm, which can readily switch from signature generation to the secret exchange of information. (The RSA can currently encrypt data at about 11 000 bits per second and decrypt it at 1100 b/s.) Its export from the United States to any country besides Canada must therefore be decided on a case-by-case basis.

McNulty said NIST wants to be able to electronically exchange keys as part of the DSS package. (Alternatives may be to couple DSS with RSA or to use a Diffie-Hellman technique called mutual key establishment, which lets two users cooperatively generate keys without exchanging secrets. Both, however, are patented and "everyone wants NIST to come up with royalty-free standards," Branstad said. There are unresolved charges that the DSS itself infringes on several existing patents, including one by Claus P. Schnorr of Germany.)

Still, because the RSA is already in several international standards and is a *de facto* standard in U.S. industry, many in industry are questioning why a new standard is needed. Industry giants such as AT&T Co. and IBM Corp. have advocated encryption standards compatible with worldwide systems, in effect backing the existing RSA approach. (During Congressional testimony in May, IBM opposed a DSS, calling it an "unproven methodology" and saying it would force users to buy multiple products to implement differing techniques.)

Branstad admitted it would be more work for industry to support two standards, primarily in the overhead of maintenance, training, and so on. But, he added, "More and more people are discussing the use of DSS," including some large standards agencies. NIST's McNulty acknowledged that "we realize RSA will still be around."

Companies already adopting the RSA public-key system include Microsoft, IBM, Sun Microsystems, Lotus, Novell, Digital Equipment, Motorola, Northern Telecom, Exxon, Citicorp, Boeing Computer Services, Dupont, General Electric Information Systems, and Apple. The first three adopted RSA after the DSS was proposed. Standards works that involve RSA include: International Standards Organization's X.500, for electronic directories; Etebac-5, for French Banking; AS2805.6.5.3, the digital signature standard for Australia.; and RFC1114, for Internet privacy-enhanced mail.

Walker, the ex-Pentagon director of information systems, said: "RSA is already so widely established that deviations from it will be highly counterproductive."

The third DSS weakness is simply one of perception. The credibility of NIST, as industry's advocate in Government, is questioned. For various reasons, the process by which DSS was derived was much more secretive than that of the DES in the 1970s. The real issue may not be whether the DSS is a good algorithm, but the fact that its de-

The debate over the U.S. digital signature standard (continued)

from manufacturing and using encryption equipment within this country or for use by the U.S. firm or its subsidiaries in locations outside the United States because of U.S. export restrictions. In fact, NSA has always supported the use of encryption by U.S. businesses operating domestically and overseas to protect sensitive information.

For export to foreign countries, NSA as a component of the Department of Defense (along with the Department of State and the Department of Commerce), reviews export licenses for information security technologies controlled by the Export Administration Regulations or the International Traffic in Arms Regulations. Similar export control systems are in effect in all the CoCom countries [Coordinating Committee on Export Controls, embracing Japan and most West European nations] as well as many non-CoCom countries, as these technologies are universally considered to be of strategic national concern and therefore sensitive.

Such technologies are not banned from export and are reviewed on a case-by-case basis. As part of the export review process, licenses may be required for these systems and are reviewed to determine the effect such export could have on national security interests—including economic, military, and political security interests. Export licenses are approved or denied based upon the type of equipment involved, the proposed end-use, and the end-user.

Our analysis indicates that the United States leads the world in the manufacture and export of information security technologies. Of those cryptologic products referred to NSA by the Department of State for export licenses, we consistently approve over 90 percent. Export licenses for information security products under the jurisdiction of the Department of Commerce are processed and approved without referral to NSA or DOD [Department of Defense]. This includes products using such techniques as the DSS and RSA which provide authentication and access control to computers or networks.

In fact, in the past NSA has played a major role in successfully advocating the relaxation of export controls on RSA and related technologies for authentication purposes. Such techniques are extremely valuable against the "hacker" problem and unauthorized use of resources.

. . . and experts reply

RONALD L. RIVEST: NSA's reply to this question [on the origin of DSS and the possibility of trapdoors] is misleading in a number of respects, and avoids discussion of a key issue: who makes the moduli for the keys? This reply also makes some fundamental mistakes in its comparison of RSA with DSS, indicating a lack of understanding of the issues or of the technology.

The trapdoor issue has to do with trust: is it possible for the creator of a DSS modulus (a large prime number) to construct the prime so that he can later [calculate the secret key and] forge DSS signatures of anyone using this prime?

This is considered an open research question in the field of cryptography. The possibility of building trapdoor primes for DSS has apparently taken NSA by surprise, enough so that they are now recommending a modified procedure for generating primes. (I have not seen their proposed procedure, and cannot comment on whether it seems satisfactory.) Given that the whole issue of trapdoor primes is relatively new, a consensus of active cryptographers on the security of any particular approach may take a while to develop.

I believe it is essential, therefore, for any users of the proposed DSS to use primes they have generated themselves. . . . The problem of a trapdoor only arises when you are trusting someone else to generate the modulus.

The NSA reply states: "the alleged 'trapdoor' vulnerability is true for ANY public-key–based authentication system, including RSA." This is false. The issue of a trapdoor only arises when the user's modulus is generated by another person. With RSA, every user generates his own modulus, so he doesn't need to trust someone else to correctly generate a trapdoor-free modulus for him. It is just not possible for an RSA user to insert a "trapdoor" into his own modulus—this makes as much sense as forging one's own signature.

The NSA reply states that "with the DSS the primes are PUBLIC and therefore subject to public examination." The implication here is that public examination of the prime modulus is somehow an advantage, compared to (say) RSA, where the primes are hidden from view. But surely, the less information one gives to a potential adversary, the more likely one is to obtain security. Knowing that the modulus (p) is prime, and knowing a large factor (q) of (p–1), may be very useful for an adversary. Indeed, a variant of DSS-like schemes in which the modulus is the product of two large primes (as it is in RSA) could easily prove more secure than the proposed DSS.

On the positive side, the increase in the allowed modulus size to 1024 bits is a definite improvement over NSA's initial proposal. And I also agree with their emphasis on the need for proper implementa-

velopment typifies a Government culture that many believe needs to be changed.

CRYPTO CURBS. U.S. export controls, because they are driven by the historic premise that cryptography should be the domain of the national security interests, are more restrictive than in many other countries, Walker said. The Pentagon and NSA veteran added that "many individuals in the national security community who are insisting upon these export control restrictions do not really understand the global impact of what is happening" in the commercial world. He told Congress that recent U.S. government-funded research projects have been prohibited from citing openly published technical articles on RSA, whereas European industry is publishing hundreds of pages in open literature a year. [See "The NSA speaks. . . ," for its view on export controls, pp. 32–35.]

The U.S. government cannot halt the spread of cryptography, said Addison M. Fischer, president of Fischer International Systems Corp., Naples, Fla., a large supplier of information security systems. RSA public key technology is fully described in millions of textbooks throughout the world, he said. Demand will be satisfied, he added, with or without U.S. products.

DES is also a worldwide standard, Fischer noted, but because of export restrictions, U.S. producers cannot sell products using DES to non-U.S. foreign companies, except banks or subsidiaries of U.S. companies. The void is filled by non-U.S. companies. Similarly, many non-U.S. companies can brandish corporate-wide global solutions, while U.S. companies are limited to offering a U.S.-only solution.

"Incredible as it may seem, mass market software programs with encryption capabilities—the kind of shrink-wrapped boxes you can buy in thousands of stores—are currently treated as 'munitions' for export licensing," said Microsoft's Myhrvold. Besides being easily carried out of the country in a briefcase, the programs can be transferred overseas electronically by modem. That being the case, the controls do not affect national security—they only impede global U.S. competitiveness, he told Congress in May. Criminal penalties include fines of up to $1 million and up to 10 years in prison.

DES and RSA are becoming widely used in Europe, where government restrictions are less severe than in the United States, said Walker, who helped write the influential 1991 report by a council of the national academies of Science and Engineering, Washington, D.C. He said the U.S. export controls are curbing development of the domestic information security market, because many U.S. computer vendors would rather make a single easily exportable product.

Eventually, Walker believes, decisions at the Presidential level will be needed to balance economic interests with those of national security. But for that to happen some issues must be aired first by the community of those immediately affected.

tion and use of any signature scheme—the differences between DSS and RSA are irrelevant if the user can't keep his secret key secret.

In summary, it seems that NSA is responding positively to the legitimate concerns that have been raised about the lack of security in the proposed DSS, including the possibility of trapdoors. Their "patches" to the original proposal may overcome the observed defects. However, some time will be required for the cryptographic community to study and evaluate these proposed changes.

D. JAMES BIDZOS: NSA's statement [about export laws], in my opinion, demonstrates that it simply does not understand, or chooses to ignore, the concerns being raised by industry.

NSA states: "We are unaware of any case where a U.S. firm has been prevented from manufacturing and using encryption equipment within this country. . . because of U.S. export restrictions."

The reality is that no major product developer can justify building a product for sale only in the United States and to U.S. subsidiaries overseas. Therefore, these products do not get built. Virtually every major computer manufacturer in the United States derives over 50 percent of its revenues from non-U.S. sales. We bring to NSA's attention the case of Digital Equipment Corp., who designed and manufactured a secure operating system that met NSA's own highest levels of defined security. When export approval was denied, Digital determined that it was not economically feasible, in spite of its investment, to bring the product to market.

NSA says its studies show the United States "leads the world in manufacture and export of information security technologies."

Since most quality cryptography was invented here, and most computer and software manufacturers—the natural source of such systems—are located here, this is no surprise. A closer look reveals that the market outside the United States for security products is growing rapidly, but the U.S. share of that market is not, and may dwindle. As foreign manufacturers of security equipment, buoyed by their success at the expense of export-restricted U.S. companies, begin to expand their efforts, they will threaten U.S. companies here in the import-unrestricted U.S. domestic market.

A lead business story in Australia's *Courier-Mail* reported on May 18 that U.S. export controls will be directly responsible for three Australian companies taking over US $100 million per year in business in Australia alone from U.S. suppliers of Pay-TV systems. They report that the full amount could be billions in the emerging Pacific market for these systems.

Consider what may happen as cryptography finds its way into mainstream computer and software products. IBM has already lost overseas sales of mainframe systems with embedded cryptography because they could not be exported to eager European buyers.

NSA points to the relaxation on export controls for products using the digital encryption standard (DES) and RSA only for authentication, which provides useful protection against hackers but no privacy whatsever. One should ask why such uses were ever controlled in the first place.

NSA frequently responds to complaints about export controls with requests for specific instances of lost sales. At a June 1992 conference in Washington, D.C., five panelists discussed how export controls were affecting their business. One of the panelists, a representative of a Fortune 500 company, described how two of the firm's main clients were lost because adequate security could not be offered by the U.S. company in Europe. Another panelist, representing a major computer company, described how a European company was created and funded specifically to exploit market opportunities created by U.S. export controls. He further stated that his company had lost system sales—hardware and software—out of inability to provide adequate security to foreign buyers. A representative of the Software Publishers Association, representing over 900 companies, stated that its members, owing to export controls, were losing sales to foreign competitors, and that the controls were stifling innovation.

Unfortunately, NSA, although invited, declined to attend this conference. (To its credit, the State Department was there.)

These are some of the warning signals that the current policy should be reviewed, with input from industry. By the time the damage is indisputable, markets will have been lost. With DES and RSA published in technical journals, on computer bulletin boards, and in textbooks around the world, the failure of current controls is inevitable.

The U.S. computer and software industries lead the world. Much of this success can be attributed to innovation, an entrepreneurial spirit, and the ability to bring new technologies to market ahead of foreign competitors. Current export controls discourage the very behavior that plays such a large role in our success.

Most of the computer industry understands that NSA has legitimate national security concerns that make its job of balancing interests difficult. What frustrates them is that NSA refuses to recognize or even acknowledge the real problems they face as a result of NSA policies.

Bad code

The 517th anniversary of Michelangelo's birth brought world attention to programs meant to harm rather than help users

On March 6, 1992, a computer virus dubbed Michelangelo damaged software on some 2000 personal computers worldwide by randomly overwriting their hard disks. The mess could have been much worse; USA Research, a marketing research firm in Portland, Ore., estimated that 64 390 computers in the United States had been infected by the virus, but actual damage was limited to a few hundred systems thanks to widespread publicity and distribution of thousands of Michelangelo virus disinfectant programs. PC users were instructed to either use antivirus software to remove the virus from their systems or to advance the date on their computers past March 6 to prevent the virus from activating.

The Michelangelo virus first came to light on Feb. 4, 1991, when a personal computer store in suburban Melbourne, Australia, found that, after a program called VET had been installed on a PC being readied for shipment, it had only 639K bytes of main memory available, instead of the 640K bytes it should have had. Then it was found that the PC altered the boot sector of a previously clean disk (after a DIR command had been used to look at the disk's contents). Further analysis of the boot sector disclosed the presence of a hitherto undiscovered virus. A few days later, Max Tefler at the Chisholm Institute of Technology in Victoria, Australia, was told about this new virus, which was set to activate on March 6. As it happens, that is Tefler's birthday; he knew it was also Michelangelo Buonarroti's and so the virus was given the name of the great Renaissance artist.

Written and "released" sometime earlier by person or persons unknown, the Michelangelo virus was spread from one PC to another by floppy disks from infected systems. Several companies inadvertently shipped the virus in their software when computers in their distribution centers became infected. Intel Corp. of Santa Clara, Calif., for one, shipped 839 copies of its LANSpool 3.01 print server utility infected with the virus before it was detected. Leading Edge Products Inc. of Westborough, Mass., for another, shipped about 500 infected PCs. And Lotus Development Corp. of Cambridge, Mass., shipped some infected versions of its CD/Networker product. Once they discovered the problem, most companies sent fixes or virus eradication software to their customers; Lotus went so far as to dispatch technicians to eradicate the virus at each infected customer.

John B. Bowles and Colón E. Peláez
University of South Carolina

MALICIOUS TYPES. Michelangelo is only one of a growing number of viruses and malicious computer programs that attack computer systems. Research conducted before Michelangelo's widespread attack shows that malicious software was already having a deleterious impact on organizations. Many had already experienced losses in productivity and data due to viruses [Fig. 1].

Depending on how they are classified, viruses vary in number from less than 100 to more than 1000. In Germany, the University of Hamburg's Virus Test Center has identified more than 300 types of viruses that attack IBM-compatible PCs. Michelangelo is one strain of the so-called Stoned virus, which infects a disk's master boot record.

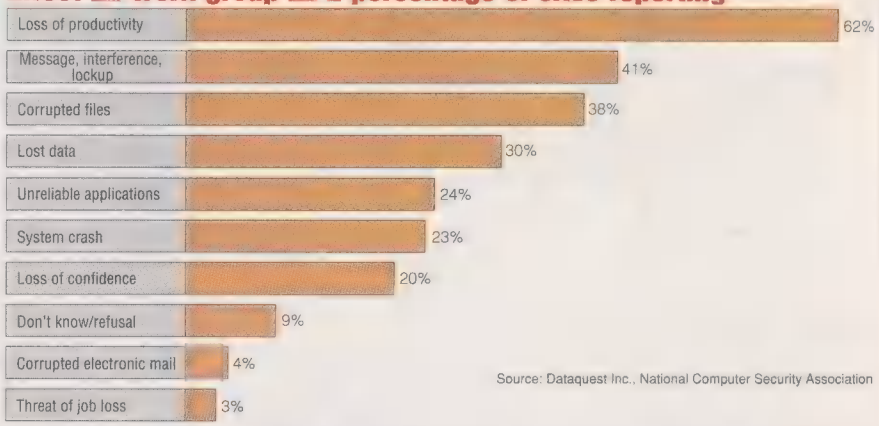
The term "computer virus" is often used in a generic sense to mean any type of malicious computer program although, strictly speaking, a virus is only one class among several [Fig.2]. Many malicious programs remain rather benign (except for occupying disk and memory space and utilizing processor time) until some trigger condition occurs, at which time they begin to destroy data and spoil system software.

Common trigger events include accessing a particular data file, the passage of a given amount of time, or the occurrence of a specific date. The most common types of damage are destroying data, imitating hardware errors, allowing unauthorized access to the system, and causing systems to crash.

TROJAN HORSES. Like its namesake from Virgil's *Aeneid* (Book II), a Trojan-horse program at first appears innocuous. Often offered as a gift, it entices users by performing a useful function. But once inside a user's computer, code hidden in the program becomes active and either executes malicious acts or creates a way of subverting system security so that unauthorized personnel can gain access to the system and/or special files.

The possibility of implanting such code in a program without modifying its source code (and thereby rendering it virtually undetectable) was demonstrated by Ken Thompson who, along with Dennis Ritchie, created the Unix operating system. In accepting the Turing Award of the Association for Computing Machinery (ACM) for his part in developing Unix, he showed how a compiler could be rigged to produce a Trojan horse while

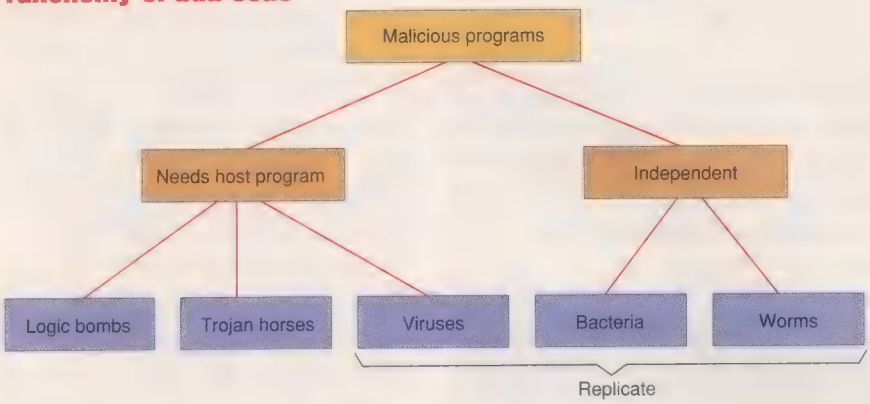
Effect on work group as a percentage of sites reporting



[1] A recent study of over 600 medium-sized to large computer-user sites, undertaken by Dataquest Inc. and the National Computer Security Association, indicates that viruses caused productivity declines at almost two-thirds of the sites and corrupted files at more than a third. Worse yet for the computer industry, one-fifth had their confidence in computers shaken.

0018-9235/92/$3.00©1992 IEEE

Taxonomy of bad code



[2] This taxonomy of malicious programs is based on their general behavior and implementation. Logic bombs, Trojan horses, and viruses reside in a host program, run only when it runs, and depend on it for their existence; bacteria and worms are independent. Viruses, bacteria, and worms replicate themselves, whereas logic bombs and Trojan horses do not.

compiling a harmless program.

Thompson wanted to alter the *login* command, the standard means of access to Unix systems, to accept either the user's password or a special password that he supplied. He could then use his special password to log into any Unix system as any user, even as the "superuser" with access to all system resources. Programmers refer to this ploy as creating a "trap door."

Rather than change the source code of the *login* command (which could be easily detected), he changed the C compiler. When the doctored compiler was used to generate machine code, it would check each line of source code until it found the *login* program. The compiler then changed that program using the code Thompson had modified to create a trap door [Fig.3]. Even though the compiled software now contained Thompson's trap door, the source code for the *login* command had not been changed and thus contained no trace of the alteration.

Even a rigged compiler's own source code need not contain the source code for inserting the Trojan horse into the *login* code. After all, a C compiler is itself a program, written in C, that must be compiled using a compiler. If the latter compiler contains the Trojan horse code, it can surreptitiously insert the code into every compiler it compiles. Thus the Trojan horse is carried to each succeeding compiler and, once the original, modified compiler has been destroyed, the malicious code does not exist in the source code of any program. Only a careful and thorough analysis of the compiler's output would result in detection of the substitution.

VIRUSES. Viruses are small programs, typically less than 2 or 3 kilobytes of code, that attach themselves to other programs and usually execute as the first few instructions of the host program. They operate in two phases: a replicate phase in which the virus reproduces but has no ill effects on the host system, and an active phase in which it changes character and carries out its main function—most often, damaging its host computer system.

Most viruses include a string of characters that acts as a marker showing that the program has been infected. When a virus replicates, it randomly selects an executable file and checks to see if the marker is present. If it is, the file is already infected, and the virus selects another executable file. When the virus finds an uninfected program, it inserts a copy of itself into that program. In this way, the virus avoids multiple infections that would cause an object file to grow ever longer, and can infect many programs without noticeably increasing disk space usage.

During its replicate phase, the virus tries to infect as many programs as possible. Since the virus can perform its mischief only when an infected program is run, infecting multiple programs makes it more likely that an infected program will be running when the triggering condition occurs.

Part of the virus code checks to see if the triggering condition has been met. If it has, the virus enters its active phase; otherwise control is passed back to the original program. Examples of triggering conditions are a program being run a certain number of times or the system clock reaching some date. (Friday the 13th and April Fool's Day are popular choices.)

In the active phase, many viruses incorporate some kind of manipulation task that reveals their presence. Typical manipulations include unusual or amusing screen displays [Fig. 4], unusual sound effects, simulating hardware failures, system reboots, altering numeric data in spread sheets, erasing files, or even reformatting the system's hard disk.

Three architectural features make IBM PCs and PC-compatible computers peculiarly susceptible to virus infections. First, they lack memory protection hardware, allowing every program to have full access to all of the system's resources. Second, the software compatibility provided by DOS makes it possible to run one program in many different computer configurations. Third, accessing and reconfiguring the interrupt system and Basic Input Output System (BIOS), which are stored in RAM, is easy.

When first turned on, PCs go through a

Fiction infects reality

The first use of the term "virus" to describe a program that infected a computer was apparently by David Gerrold in his science fiction, according to Eugene Spafford, an assistant professor at Purdue University's Department of Computer Sciences, West Lafayette, Ind., whose report on the Internet worm appeared in the January 1989 *ACM Computer Communication Review.* Gerrold's short stories about the G.O.D. machine—an artificially intelligent computer whose software "consciousness" was nicknamed Harlie—were published from 1969 on and later incorporated into the book, *When Harlie Was One* (Ballantine Books, 1972, first edition).

In one story-line, an unethical scientist created a program named VIRUS that caused its host computer to dial phone numbers at random, until it found another computer, which it would then break into and reprogram with a copy of VIRUS. VIRUS would infiltrate the software on the infected computer and slow it down so much that it became unusable. The scientist had plans to sell a program named VACCINE that could cure VIRUS and prevent infection, but disaster ensued when noise on a phone line caused the virus to mutate and VACCINE was no longer effective. The material on this fictional virus was deleted from the second edition.

The term "computer virus" was first used in a technical sense by Fred Cohen, a consultant with Advanced Security Protection in Pittsburgh, in his dissertation research while at the University of Southern California (USC), to describe a computer security problem.

Later, in a paper for the 1984 National Computer Security Conference, he defined a virus as "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself. . . . Every program that gets infected may also act as a virus and thus the infection grows." He credits the name "virus" to a USC professor, Len Adleman, the "A" in RSA encryption algorithm. The first wild IBM PC computer virus was the Brain virus from Pakistan discovered in 1986.

In *The Shockwave Rider* (Harper and Row, 1975), John Brunner described a world of computers connected by a network. Programs he called tapeworms lived inside computers, could breed by themselves, and spread from machine to machine. The name was taken up by researchers at Xerox Corp.'s Palo Alto Research Center, who experimented from 1979 to 1981 with worm programs as a way of implementing distributed computation. Their experiences are reported in an article appearing in the March 1982 *Communications of the ACM.*

—J.B.B. and C.E.P.

long process of bootstrapping, self-testing, and transferring control among the system start-up routines. Although most of these routines are stored in ROM and are thus immune to viruses, the vectoring information and parameter settings are stored by the system in RAM. Viruses can take advantage of this vulnerability for self-copying or for including jumps to their own code.

When a disk is formatted as bootable, the first sector, known as the master boot record (MBR), holds the BIOS parameters block (BPB), which contains detailed data on the layout of the file system on the disk (the file allocation table or FAT) and instructions to begin the system boot sequence. A common use of the MBR is to execute an application program automatically on start-up; unfortunately, this can also include automatic initiation of a virus. Some viruses will relocate the MBR code and replace it with their own viral code. Thus, they can gain control of the computer early in the boot process before any antivirus utilities have been activated.

Viruses often infect programs in command (.COM) files, which have an initial jump to the executable code. A virus can store this jump, and replace it with a jump to its own code. Then, when the infected program is run, the virus code is executed and, when finished, jumps to the start of the program's original code using the stored jump address.

For a virus to spread, its code must be executed either as a direct result of the user invoking an infected program, or indirectly, say, as part of the system boot sequence or as a background administration task.

Many of the known viruses remain resident in memory once their code has been executed, even though their host program has terminated. A memory-resident virus copies itself into a block of memory and modifies the standard interrupt system used by DOS and the BIOS. Then, when application programs use the interrupt system to make service requests of the operating system, they inadvertently invoke the virus. In this way, a virus may spread to all programs in the system once a single infected program has been run. This spreading occurs during the entire work session, rather than during the small period of time when the infected program executes its viral code.

LOGIC BOMBS. Logic bombs are exactly that—programs that lie dormant until some trigger condition causes them to "explode" and destroy the host computer's files. Logic bombs can be embedded in a Trojan horse or carried about by a virus. They are a favored device for revenge by disgruntled former employees, who can set the bomb to activate after they have left a company. The trigger condition may be the deletion of the dismissed employee's name from the payroll records. The "explosion" is often timed to do the maximum damage at the most inopportune moment.

This delayed-action facility has also been used for ransom demands—"pay and the place where the bomb is hidden will be revealed." In addition, suppliers and consultants who set up a computer system have used it as insurance—if their bills are not paid, the bomb can be exploded, wrecking the system. This threat was used when a Maryland library refused to pay for a system that did not function properly, but the supplier's bomb was found before any damage was done.

Logic bombs can be programmed to target specific users, as was the case of the Scores Virus—a Macintosh virus created for revenge and sabotage by a disgruntled ex-employee of Electronic Data Systems (EDS) Corp., Dallas. The program infected any application program, increasing its size, and sought out new hosts to infect every three and one-half minutes. It searched for several specific files containing EDS employee information and destroyed them and, in the process, slowed down the system, produced printing problems, and modified icon forms.

THE WORMS' TURN. Worms are programs that travel through a network from one workstation or computer to another. They were first devised at Xerox Corp.'s Palo Alto Research Center (PARC) as a tool for doing useful work on a network and distributing information, such as system configuration data, in a distributed environment ["Fiction infects reality," p. 37].

Worm programs move around by taking advantage of the way in which resources are shared on a computer network and, in some cases, by exploiting flaws in the standard software installed on network systems. A worm that is executing on one computer connected to a network searches for other potential hosts on the net. When it finds one, it establishes a communications link with the remote system and sends it a "vector" consisting of bootstrap code. The vector then establishes a communications link back to the infecting system and the new host downloads copies of the files that make up the main body of the worm.

> 'Computer virus,' often used to mean any malicious program, is but one of several such program classes

By subverting the operation of systems on the network to their own purposes, monopolizing their resources, and saturating the communications links in a network, worms are capable of crippling a network even when not overtly destructive. Often, the entire network of computers must be shut down before it can recover.

One way in which a worm propagates is illustrated by the infamous Internet Worm, which infected Unix systems on the U.S. Internet network on Nov. 2, 1988. Once the worm became established on a system, it began to collect information about other hosts to which the system was connected. It then made up to three attempts to infect those hosts. First, it tried spawning a remote shell on the target system using the Unix *rsh* (remote shell) command. If successful, it set up a transmission control protocol (TCP) connection back to the infected machine so that the vector program could be sent to the target, compiled, and executed. Then the vector worked in concert with the server worm to copy the actual worm body to the target, where it was compiled, linked, and executed. After the server worm determined that the infection had been successful, it disconnected.

If the first method failed, the worm tried to exploit a flaw in the *fingerd* program by overrunning its input buffer with a specially constructed 536-byte string. The *fingerd* process normally runs as a daemon (a Unix process not associated with any user that runs in background to take care of a system-wide function) to provide information about other users, such as a full name or perhaps a telephone number where the user can be reached. This utility uses the C library function *gets* to read input data; *gets* reads the entire input string without checking for buffer overruns. The overrun caused an area of the system stack to be overwritten, allowing the worm to put instructions on the stack that, when executed, resulted in a connection to a remote shell via TCP. The infection then proceeded as explained above.

If both the first two methods failed, the worm tried to connect to the SMTP (Simple Mail Transfer Protocol) port on the remote machine. The Unix electronic mail utility, *sendmail*, listens to this port for mail deliveries. One option of the *sendmail* program is the DEBUG command, which allows program testers to verify that mail has arrived at a site, without having to invoke the mailer's address-resolution routines. Many vendors and site administrators leave the debug option compiled into the *sendmail* code to facilitate configuring the mailer for local conditions. The worm issued the DEBUG command to *sendmail* and then enacted a sequence of commands to mail the vector to the target system and start it running. The worm body was then transferred in the same manner.

Once installed, the new worm's first actions were to camouflage its existence. It unlinked the binary version of itself, killed its parent process, read its files into memory and encrypted them, and deleted the files created during its entry into the system. It then began systematically to break into user accounts by exploiting the accessibility of the Unix password file and the tendency of users

```
Compile (s)
char *s;
{
  if (match (s, "pattern"))
    {
      compile ("bug code");
      return;
    }
  < other statements ....>
```

[3] Using this kind of routine, a compiler can search source code for a character-string and secretly insert "bug code."

to choose common words as their passwords. Once it learned a user's password, it could masquerade as the user and gain access to remote machines where that user had an account.

The worm periodically "forked" itself (a process whereby a Unix program starts a new process by creating a clone of itself) and killed its parent, so that its process ID was constantly changing. This prevented any one process from accumulating a suspicious amount of central processing unit (CPU) time, and ensured that its scheduling priority would not be downgraded for excessive CPU time. Every 12 hours, it erased its record of the hosts it had infected, thereby allowing already infected hosts to be put back on the list of potential targets. Thus, a single worm could reinfect the same host after 12 hours.

(In fact, these ploys did not always work as planned and in some cases the worm could be spotted because systems were hit with a dozen or more copies, all using up inordinate amounts of CPU time. A more bug-free worm might have lasted much longer.)

BACTERIA. The use of the term "bacterium" for malicious code is relatively new and some virus researchers prefer to include them in the virus class. Others treat them as a different class since, unlike viruses, they do not need a host program.

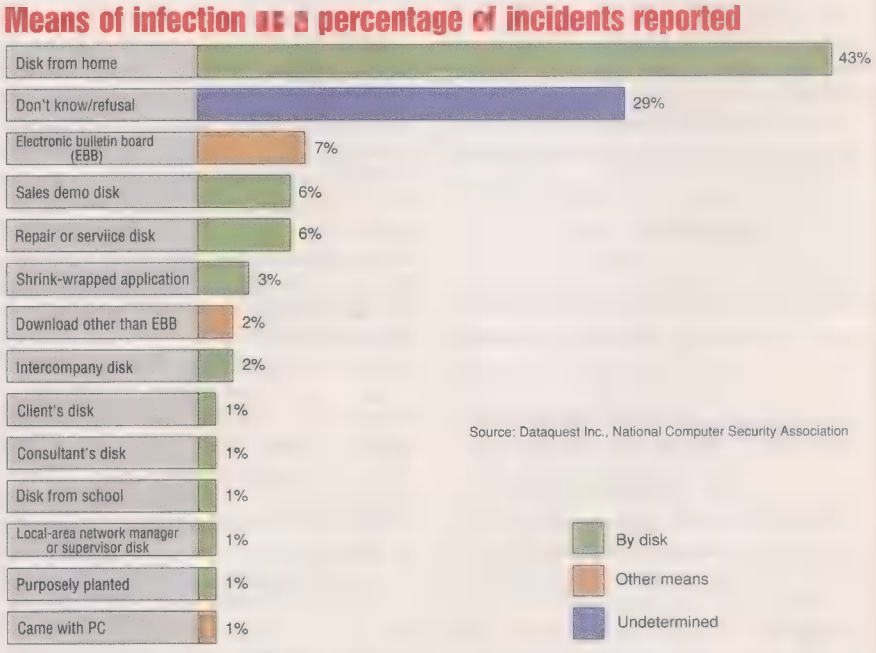
A bacterium program simply tries to replicate itself. It acquires as much CPU time as possible so as to slow down its host system (by executing many versions of itself), and it may also try to fill up disk space with copies of itself. One example of a bacterium is the IBM Christmas Bacteria which, in December 1987, invaded the Bitnet, a leased-line network of universities begun in 1981 by the City University of New York and Yale University in New Haven. The bacterium displayed a picture of a Christmas tree on the screen, while using the network electronic mail system to distribute copies of itself to every user on the mail distribution lists of the person on whose system it was currently running. Its growth was geometric, and it quickly bogged down the network, which had to be completely shut down before all copies of the program could be eradicated.

PREVENTION AND CURES. Recovering from a virus infection is no easy task. It requires a high degree of technical competence, dedicated time, and many resources. All or part of the computer system may have to be shut down for long periods of time, and essential programs and data may be lost. The longer a virus remains in a system, the more time it has to spread, and the tougher recovery from it becomes.

Worse yet, the computer may be connected to a network or another system that provides shared data and program files for multiple users. An infected file on the network server can infect every workstation on the network. If the infection is not removed from every workstation at the same time, reinfection will occur, and the cycle begin again.

All malicious programs are highly dependent on the operating systems for which they are written. Consequently, measures to prevent their execution and growth are also sys-

[4] The Cascade virus randomly selects characters from a display and causes them to "cascade" down the screen until they pile up at the bottom of the display. The photo shows a virus simulation written by Joe Hirst, British Computer Virus Research Centre, Brighton, England.



[5] A recent study shows that viruses most often spread through disks that users bring into the office from home. Use of frequently updated virus protection and eradication software would help prevent systems from being contaminated by viruses introduced in this way.

tem specific. Nevertheless, a few general guidelines can be applied.

Passwords are at the heart of most computer security systems and users would do well to pick their passwords more carefully. Many user accounts can be broken into by using the following password variations: the account name, the account name concatenated with itself, the first or last name of the user with an initial capital letter, the lower-case version of the first or last name of the user, and the reverse of the account name. A good password must not be guessable; should not be in a dictionary; should be changed regularly; and should be easily remembered. User-generated passwords rarely meet the first three criteria, and machine-generated passwords fail the last.

Programs such as *passwd* on Unix systems that enable a user to set the password should be modified to reject these common choices for a password, and passwords should expire automatically after a certain amount of time. Some systems do not encrypt user passwords and even those that use one-way ciphers provide protection only against casual snooping—not a serious attack. An intruder with access to the system password file often can learn many account passwords easily. All he or she need do is encrypt the words in the system dictionary and compare the results to the encrypted words in the system password file.

Although many systems operate in a friendly environment, administrators and privileged system users must still be concerned with system security. Changes made in the operating system for the convenience of local managers often introduce weaknesses that can be exploited by a malicious program or an intruder. Practices of this type include altering search paths to make it easier for system programmers to use the system while running as the superuser; providing write access permissions to system directories; setting up permission files to ease file transfers between systems; and using shell scripts to connect and log on to remote systems. Once a system is set up, a more secure operating procedure is to require that a password be entered before allowing any system program to be altered or a new program to be installed. File transfers should also be accomplished by means of a password rather than with permission files.

System users should also be trained to take a more proactive approach to security. A recent study indicates that most viruses are transferred by disk that users put—or let others put—in their systems [Fig. 5].

Practices analogous to those used to safeguard food and drugs are helpful; users should refuse to accept software in unsealed packages or from untrusted sources. They should never borrow a program from someone whose security standards are less rigorous than their own. They should regularly use programs that check for known viruses and update these programs frequently. They should be wary of public domain software, software obtained from bulletin boards, and programs sent by electronic mail. They should develop the habit of monitoring the last-modified dates of programs and files in their own systems.

Surprisingly, one common means of spreading viruses is in the disks used to diagnose computer troubles. Several viruses simulate hardware problems. Thus, an infected computer may appear to be having a hardware problem. To diagnose the problem, a technician will insert a diagnostic disk into the machine. The disk will become infected and when it is later inserted into another computer it will be infected also. Consequently, these disks should be checked for virus infections after each use.

> Ironically, one way viruses are spread is through the disks used to diagnose computer troubles

Once a virus has been released into a computing environment, reproduction proceeds unchecked and precautions, such as system backups, are largely ineffective since the trigger can occur months or even years after the initial infection. Restoring the system from a backup may simply reinfect it.

DISINFECTANTS. In many cases, disinfection utilities will remove a virus from a system. These programs first try to identify the specific type of virus by matching its marker, then applying a detailed knowledge of its infection method and program structure to restore the original program.

For example, in the case of viruses that modify jump instructions at the beginning of the host program, recovering can be as simple as restoring the original jump to the start of the host code. The best disinfection programs can identify several hundred viruses and are updated frequently as new viruses are discovered.

Often, however, the simplest way to "cure" an infected computer is to shut it down, purge its memory and all its disks, and rebuild its files from scratch. Programs should be loaded from the original manufacturer's copy, and new disks should be carefully screened for the presence of an unwanted intruder.

Several immunization schemes have been implemented as "vaccines" against viruses and Trojan horses. Vaccination works by modifying each program in the computer to include a self-test mechanism. The mechanism uses a checksum or other algorithmic technique to determine if the sequence of instructions within the program has been altered. This self-test executes each time the program runs, checking to see if any changes have been made to the program since it was last executed.

The most effective self-tests use public-key encryption and digital signatures to compute a checksum on object files signed by their owner using his or her secret key ["Cryptography = privacy?," pp. 29–35]. The operating system can check the authenticity of the files using the owner's public key; programs infected by a virus would fail to pass.

Other approaches for maintaining systems focus on frustrating the destructive acts attempted by malicious programs. To control file deletion or program modification, for instance, the operating system can be made to query the user for permission whenever a program attempts to make a permanent change in another program or file. However, this can become cumbersome and it is ineffective in many cases because the user of a large program (such as a word processor) may not know what files can be legitimately changed.

Memory-protection hardware that restricts a program to a limited region of memory may reduce the chances of attack. However, some viruses can still propagate in legitimately accessible programs, including portions of the operating system.

One effective technique for detecting virus infections is a "snapshot program," which logs all critical system information at the time of the initial installation. Then a check routine is run periodically to compare the system's current state with the original snapshot. If signs of infection are detected, the affected area of the computer is identified and the user is notified.

Also helpful is the "branch address maps" technique, which is used to check executable programs for signs of infection. A branch address map tracks the limits of the address space associated with all programs' service requests, such as calls to the operating system and system interrupts. This technique can verify hundreds of programs in seconds.

ABOUT THE AUTHORS. John B. Bowles (SM) is an associate professor in the electrical and computer engineering department at the University of South Carolina (USC), Columbia, where he teaches and does research in the area of reliable system design. Before joining USC, he was project leader of the Systems Analysis Group, Advanced Systems Development, at NCR Corp. and a member of technical staff at Bell Laboratories.

Colón E. Peláez is a Ph.D. student in electrical and computer engineering at the University of South Carolina and a member of the faculty at Escuela Superior Politécnica del Litoral (Espol) in Guayaquil, Ecuador. He was a technical assistant at Centro de Servicios Computacionales (Cesercomp) of Espol, responsible for the maintenance of a PC network.

A security roundtable

Using electronic mail, experts ponder whether tighter rules, a security 'czar,' or a better-informed public will ensure security

In order to look at some interrelated aspects of the security and vulnerabilities of information technologies, IEEE Spectrum *invited a few outstanding security authorities to participate in a colloquy by electronic mail.*

This was the magazine's first international e-mail conference (the first national one took place in 1983), made practical by the growth of the Internet. It took place over three weeks, from mid-May to early June.

Spectrum*'s senior associate editor in Washington, John A. Adam, organized and moderated the conference with help from participant Lance J. Hoffman of George Washington University. The computing center of the university's School of Engineering created the automatic distribution system used to post correspondence to all participants.*

What follows has been heavily edited (and reviewed by the participants) to provide only highlights selected by Spectrum. *The complete text is to be available at cost from George Washington University [for detained information on obtaining the complete text, see To probe further, p. 44].*

Taking part were:

Klaus Brunnstein, professor for applications of informatics, University of Hamburg, Germany. He founded its Virus Test Center, which now serves Germany's information security agency as a computer emergency response team. Active in national politics, Brunnstein served briefly in Germany's parliament, the Bundestag.

William J. Caelli, who directs the Information Security Research Center at Queensland University of Technology, Australia. He is also technical director of Eracom Pty. Ltd., which develops encryption and security computer systems. Caelli is chairman of the security committee of the International Federation for Information Processing Societies, Geneva, Switzerland.

Lance J. Hoffman, professor of electrical engineering and computer science at George Washington University, Washington, D.C. General chair of the Second Conference on Computers, Freedom, and Privacy held in Washington, D.C., in March 1992, Hoffman currently chairs the subcommittee on Security and Applications of the IEEE Committee on Communications and Information Policy.

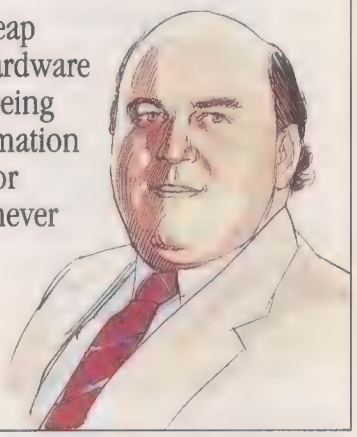
Peter G. Neumann, a principal scientist in the Computer Science Laboratory at SRI International, Menlo Park, Calif., since 1971. He is chairman of the Association of Computing Machinery's Committee on Computers and Public Policy. At Bell Laboratories he helped design the Multics secure operating system.

Marc Rotenburg, a lawyer with a technical background who directs the Washington, D.C., office of the Computer Professionals for Social Responsibility.

Willis H. Ware, a member of the corporate research staff at RAND Corp., Santa Monica, Calif. One of the original members of John von Neumann team on the Electronic Computer Project, he has been involved, at the request of the U.S. government, in the creation of official reports, one of which prompted the Federal Privacy Act of 1974.

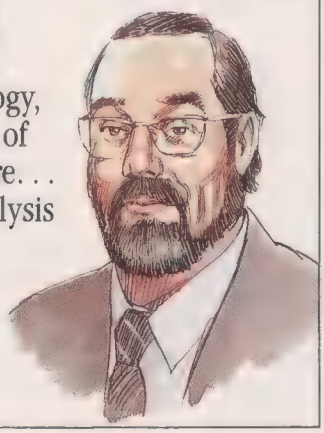
"Because of cheap initial pricetags, hardware and software are being employed in information systems for uses for which they were never designed."

William Caelli, Information Security Research Center, Queensland University of Technology, Australia



[On data security] "We are in the Dark Ages of this technology, because no designer of any essential software... did a reasonable analysis of the risk of an implementation."

Klaus Brunnstein, Virus Test Center, University of Hamburg, Germany



SPECTRUM: Research and development in computing and electronics seems to focus on speed, capacity—and openness. Is an architecture evolving that is itself increasingly vulnerable to malicious actions? If so, what are the dangers?

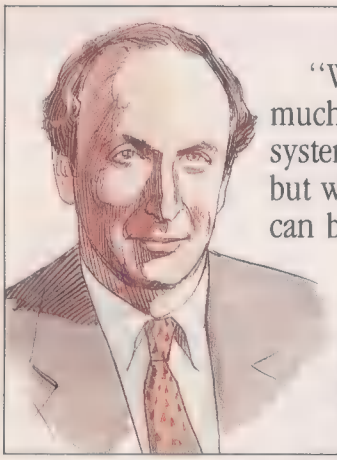
HOFFMAN: We are building much more capable systems than ever before; but when they fail, results can be catastrophic.

One problem is that there is no standard, or even general agreement, on whether to design (and pay for) very resilient systems and/or systems designed for the average case and/or systems that function fine only as long as all the manufacturer's warnings are observed and the manuals are read. When you interconnect systems of various security levels into a network, you get great utility, but security is much harder to enforce.

NEUMANN: We are increasingly relying on computers to solve problems that are not technologically based or that are beyond our abilities to solve with any reasonable assurance [of success]. Furthermore, we increasingly rely on people to solve problems that they cannot adequately solve, and to operate computer systems whose human interfaces are outrageously inappropriate for human use. Approximate solutions—particularly quick-and-dirty ones—tend to become institutionalized.

From the point of view of preventing computer misuse, including penetration by out-

0018-9235/92/$3.00©1992 IEEE



"We are building much more capable systems than ever before; but when they fail, results can be catastrophic."

Lance J. Hoffman, George Washington University, Washington, D.C.

siders and malicious use by insiders, the computer systems are inadequate, the operational system management is inadequate, and the problem is much more serious than is generally recognized.

The dangers are far more serious than just those implied by computer and communications security problems. Human safety, real-time control, guaranteed performance, and application survivability are closely related, and tend to depend on one another as well as on security—but are inadequately managed. System behavior is characteristically unpredictable and undependable.

Good software engineering practice is widely ignored. Hardware is becoming very cheap, which gives us the opportunity to use it in more challenging applications, which in some cases further increases the risks. Much greater conservatism is necessary in using computers in life-critical environments.

BRUNNSTEIN: Experience demonstrates that the threat to economies and society is becoming more serious as information and communication technologies reach a wider number of users, many of whom are untrained.

Essential terms—such as "information," "functionality," "security," and "safety"—are, if defined, differently understood. Among security experts, the concept of ▪ "trusted system" is well-defined: [it is] the Bell-LaPadula model, which is the basis of the Department of Defense's *Trusted Computer System Evaluation Criteria* (TCSEC) and *Trusted Network Interpretation of TCSEC* (TNI), and an essential part of the European Community's *Information Technology Security Evaluation Criteria* (Itsec).

But many users do not adhere to these criteria. Otherwise, nobody would use a relatively insecure system such as personal computers for work that has a legally prescribed demand for security—for instance, the storage and processing of personal data.

Professional societies need to improve upon and disseminate knowledge of the risks inherent in present concepts and usage in computing, while working to improve basic paradigms of the information architectures.

CAELLI: In the 1970s, information systems were more likely to be created around mainframe computers and data networks, which had high levels of engineering control in their development, manufacture, and support. Today, an architecture is emerging based on systems designed to be cheap and affordable.

Because of cheap initial pricetags, hardware and software are being employed in information systems for uses for which they were never designed. For example, the PC and its DOS (a totally insecure operating system) were not created as a corporate, shared workstation. The local-area network was envisioned as a high-speed link between users and systems that trusted one another.

Even when security features were made available in the hardware (for instance, the Intel iAPX-286 microprocessor protection features in the IBM PC/AT), they were ignored by the software developers.

Public and private enterprises of all sizes worldwide are now dependent on such computerized information systems. It is a recipe for disaster. Life and limb may depend upon computers embedded into cars, trucks, planes, and trains, as well as in medical diagnostic equipment and so on. We know this, but what action is being taken?

SPECTRUM: Does all this imply we should return to flying aircraft "by the seat of our pants" and to timesharing on mainframes? Compared with the car, which contributes to about 50 000 deaths each year in the United States alone, this concatenation of computers seems relatively safe.

NEUMANN: Am I suggesting we go back to the Dark Ages? Not at all, but a little reality is needed. We must recognize the risks in trusting computers and communications systems to do jobs that we ourselves cannot do reliably on the scale and with the timeliness that are demanded. And if we understand the real risks, we may decide that certain applications are just not worth it.

HOFFMAN: Isn't it unrealistic to expect system developers to refrain from applications that are too dicey, if either the profit motive or technical challenge is there? Once systems start being developed, they tend to be hard to shut off (in government or private endeavors).

On the other hand, if there is a "czar" who decides what systems are too risky to develop, don't we start trampling freedom and take decisions away from the marketplace? How do we resolve this dilemma?

NEUMANN: Why must we postulate the existence of ▪ czar? Each field tends to have its own regulatory groups, whether they are governmental, or corporate, or even self-defensive in anticipation of lawsuits.

If repeated accidents and subsequent lawsuits drive the manufacturer of ▪ particular aircraft system or the Therac 25 therapeutic radiation device [whose incorrect programming resulted in patients receiving overdoses] out of business, how is that trampling freedom? Freedom to kill people? It seems to me that some regulation is essential, to prevent fly-by-nighters from flying by the seat of their pants.

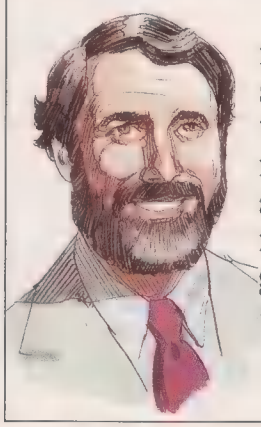
But ultimately, the profit motive cannot remain as the overriding Occam's razor for whether someone can get away with marketing a life-critical system that is intrinsically not safe.

BRUNNSTEIN: Peter, we *are* in the Dark Ages of this technology, because no designer of any essential software (not even what experts call critical software) did ▪ reasonable analysis of the risk of an implementation. I think the methodologies are nonexistent. We only learn how to assess a risk after having experienced it! Do you know of a single case where a designer of ▪ moderately complex system has been prosecuted for inadequate design?

With less than 50 years of computing experience, we may hope that future architectures may improve, whether by insight through mistakes or by superior insight in the form of some authoritarian czar. I suggest ▪ third solution: if users take ▪ more active role in design, some of the worst flaws may be overcome. (Moreover, some reduction in the rapid developments of information technology might also reduce the manifold risks!)

CAELLI: Yes, the increased distance between users and creators of the products is ▪ big problem.

We also might consider whether all professionals, just like artists, should sign their



[On preventing computer misuse] "...the computer systems are inadequate, the operational system management is inadequate, and the problem is much more serious than is generally recognized."

Peter G. Neumann, Computer Science Laboratory, SRI International, Menlo Park, Calif.

work. (Remember all the signatures on the case of the first Apple products?) This way we get to know the who of information systems design and production and not just, "Oh well, it came from Microsoft in Seattle." I want to know exactly who wrote the Windows 2 code, DOS 4.01, etc.

NEUMANN: Klaus, in 1989, a U.S. Court in Missouri held Ernst & Whinney, a major accounting firm, liable for procuring an unworkable turnkey computer system for a client, Diversified Graphics. But lawyers quoted in articles had mixed views on whether future rulings might apply to systems designers or programmers, and not just systems acquisition.

BRUNNSTEIN: Prevalent in Germany are *Vorschlagswesen* [recommendation organizations]. They are a useful means of prompting employees to improve products and processes by offering awards each year for the best suggestions. But what sort of organization is appropriate for information systems? Some sort of "anti-czar," for instance, a Ralph Nader of information technology, may be useful or even required to start the whole process of public consciousness.

HOFFMAN: I am fascinated by the idea of an anti-czar. Suppose an advocacy group, such as the Electronic Frontier Foundation (EFF) or the Computer Professionals for Social Responsibility (CPSR) had enough money and will to target, say, either a dirty dozen of particularly insecure applications or an honored circle of particularly beneficial, well-designed secure applications?

BRUNNSTEIN: I had thought those groups mainly stimulated the consciousness of experts (who also need schooling in the risks of information technology), rather than the public.

The public may easily be roused against producers of "insecure" products if the impact is easily understandable and demonstrable. Comparing Nader's activism to improve automobile security to improved security of PCs and networks, I assume that the critical mass of user awareness has probably been reached (the Michelangelo virus hysteria may indicate this), but user consciousness is not yet at the minimal level for activism.

NEUMANN: In the United States, we live in an era of Federal deregulation—and look at the air traffic control problem, the savings and loan scandal, etc. The British have bitten the bullet with Ministry of Defence standards Defstan 00-55 (*Requirements for Procurement of Safety-critical Software in Defence Equipment*) and 00-56 (*Hazard Analysis and Safety Classification of the Computer and Programmable System Elements of Defence Equipment*), which may help a little. They distribute some responsibility for evaluating software safety and system security to the civilian sector. Ultimate certification is still within the organization that has responsibilities and faces legal actions if problems ensue.

I am not for total government control, but total deregulation is a disaster, especially in a society where turning a profit is the only real bottom line.

CAELLI: Was it the car manufacturers who insisted upon seatbelts? Did building owners insist on fire sprinklers and extinguishers? NO! It took legislation for anything to really happen.

It appears the computer and software industry needs the same push. Manufacturers of hardware and software simply say: "We listen to our customers and they are not asking for security and definitely will not pay for it!"

An answer may lie in the interconnection of computers. Engineers must now stop, pause, and rethink the interconnection parameters so that security becomes a basic component. Unfortunately, there are signs that national and international computer networks are indeed being created that are vulnerable to malicious and accidental problems.

The time has come for the acceptance of quality, security, and reliability guidelines and possibly mandatory standards in networks. Legislative control is essential in security. Is information technology different in this respect from chemical or nuclear engineering? No!

BRUNNSTEIN: Current regulations—for example, TCSEC in the United States and Itsec in Europe—are not adequate to protect users against insecurities in computing. Both sets of government criteria classify information technology products on the same basis, and industry merely reflects these classifications (for instance, access control). Neither regulation classifies the negative impact of unreliable or untrustworthy systems on users' work. Moreover, classification is based on military concepts, which are not valid in most commercial applications.

Again, as "techies" concentrate on system functionalities and performance too much, consumer-oriented codetermination (regarding social aspects, human-machine interaction, reliability, trustworthiness, privacy, and so on) should be helpful.

HOFFMAN: I'd like to see not only more of that, but the reward structure changed for the techies, so that they must consider other values beyond making something work.

This is probably impossible, given the relative weakness of the professional societies in designing such things as ethics codes and enforcing them. Where are the agents of change?

ROTENBURG: These all sound like nice ideas, but there are a lot of difficult problems in the public policy world with information technology issues.

No one really cares. Really. They are not dumb, but they have other things to worry about, jobs, family, community, traditional politics.

Issues are complex. Even for interested persons, if you haven't spent a few years at Bell Labs, designed software for an airliner, or an elevator for that matter, you're basically out of the play.

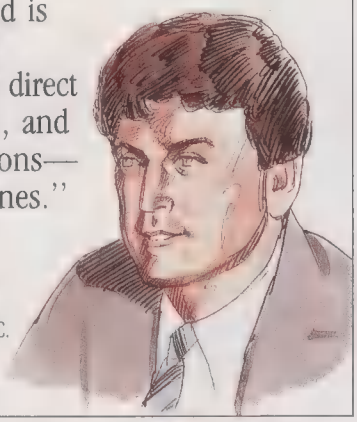
It's not clear what to do. Legislators are not dumb either, and will generally try to do the right thing. But throw two experts up at a Congressional hearing with conflicting views and you've got a policy circus.

What is needed is to make issues relevant, be direct about the problem, and put forward solutions, even incomplete ones. The policy process doesn't work without answers.

WARE: Let's keep things in perspective. We try to argue complexity is at the root of our problems. To some extent, true, but other systems have become complex and are not well understood either. Witness the rolling blackouts of the eastern United States

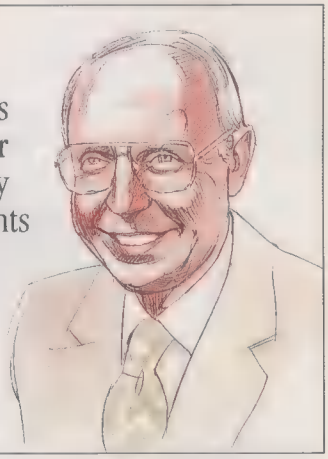
"What is needed is to make [security] issues relevant, be direct about the problem, and put forward solutions—even incomplete ones."

Marc Rotenburg, Computer Professionals for Social Responsibility, Washington, D.C.



[On Federal regulations] "What is different. . .about our technology, especially software, that warrants unique treatment by society?"

Willis H. Ware (F), RAND Corp., Santa Monica, Calif.



some summers ago, events mainly triggered by analog sensors, which interacted among themselves in ways not foreseen.

Are we asking computer-controlled products to do better than equivalent earlier products? What is different—if anything—about our technology, especially software, that warrants unique treatment by society? We complain about poor-quality software, but the market abounds with poor-quality goods and commodities—and the mechanisms to protect consumers in society.

Maybe we don't know yet how to put the equivalent of a safety factor in software. The information technologies that we love and cherish (and even feel the parental obligation for) has suddenly stepped out into full public view. And it is having the same pubescent, perhaps adolescent, trouble in responding to the full obligations of societal responsibility, criticism, and expectations.

Indeed, nothing is so pervasive in society as information. Energy allows things to exist; information allows them to behave purposefully. Maybe our business does need extraordinary treatment to avoid harming society or putting it at an unprecedented risk. Do we need some regulation in the spirit of building and housing codes? Maybe.

The onus is on us who understand it to make the case that information technology is truly unique—truly impossible to accommodate within existing means—before we promote heroic but superfluous solutions.

ACKNOWLEDGMENT. Barry Ross provided the portraits. ◆

To probe further

GENERAL. The IEEE Computer Society and IEEE Communications Society have many pertinent resources in terms of magazines and conferences on computer security. A frequently cited technical source is the *Proceedings* of the annual IEEE Symposium on Research in Security & Privacy. The most recent (1991) edition may be ordered from the IEEE Service Center, Customer Service Department, 445 Hoes Lane, Box 1331, Piscataway, N.J. 08855-1331; 800-678-IEEE. Previous *IEEE Spectrum* reports in this area include "The quest for intruder-proof computer systems," August 1989, and "Can computer crime be stopped?," May 1984.

The U.S. National Institute of Standards and Technology (NIST), Gaithersburg, Md. 20899, publishes many concise reports on information security and offers help in creating incident-response capabilities. Much is accessible from the NIST Computer Security Bulletin Board at 301-948-5717 (for 2400 baud or less) or 301-948-5140 (for 9600 baud). Its Internet electronic-mail address is csrc.ncsl.nist.gov.

The NIST and the U.S. National Security Agency sponsor the annual National Computer Security Conference. This year it will be held Oct. 13–16 in Baltimore, Md.

Computers at Risk: Safe Computing in the Information Age (National Academy Press, 1990) by doyens of U.S. industry, including *Spectrum* roundtable participants Peter G. Neumann and Willis H. Ware, is a valuable resource. It prompted the creation of the International Information Security Foundation (I²SF), temporarily based at SRI International, Menlo Park, Calif.

The Information Technology Association of America, 1616 North Fort Myer Dr., Suite 1300, Arlington, Va. 22209 (703-522-5055), has position statements on changes recommended on information security policy, mainly commenting on the aforementioned report. It is also active in the I²SF creation.

"Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information," October 1987, by the U.S. Congressional Office of Technology is still a good basic resource. It is available from the U.S. National Technical Information Service, 5285 Port Royal Rd., Springfield, Va. 22161; 703-487-4650.

The Computer Security Information Resource is another on-line information system (fax, 415-495-4642), which is currently free of charge. It has joint projects with the National Computer Security Association to disseminate information and the National Center for Computer Crime Data, Santa Cruz, Calif. (408-475-4457) to develop a database of crime. Both are private organizations.

The Computer Security Institute, 600 Harrison St., San Francisco, Calif. 94107 (415-905-2626), and the National Computer Security Association, 227 West Main St., Mechanicsburg, Pa. 17055 (717-258-1816), hold several conferences annually and offer other general services.

The full transcript of *Spectrum*'s roundtable electronic mail discussion is available for US $7 from Sherifa el-Zeneiny, Department of Electrical Engineering and Computer Science, George Washington University, 801 22nd St., Suite T634, N.W., Washington, D.C. 20052.

Information Security Handbook (Macmillan, 1991), by roundtable participant William Caelli et al., is a general resource.

VIRUSES. *Computers Under Attack: Intruders, Worms, and Viruses*, edited by Peter J. Denning (Addison-Wesley, 1990), is a collection of 40 landmark papers on threats to the privacy and integrity of computer systems. *Rogue Programs: Viruses, Worms, and Trojan Horses* was edited by roundtable participant Lance J. Hoffman (Van Nostrand Reinhold, 1990). It contains 27 articles judged to be the best on the subject by a seminar of computer science graduate students. Some of the same article are in Denning's book.

The most recent technical book on computer viruses is David J. Ferbrache's *A Pathology of Computer Viruses* (Springer-Verlag, 1992), while a seminal work on the topic—which also covers early virus history—is Fred Cohen's Ph.D. dissertation, *Computer Viruses* (University of Southern California, 1985, available from ASP Press, Pittsburgh). An interesting paper on recent research viruses, "An Overview of Computer Viruses in a Research Environment," by Matt Bishop, appears in the *Proceedings of the Fourth Annual Computer Virus & Security Conference* (Data Processing Management Association, 1991).

Computer Viruses and Anti-Virus Warfare, by Jan Hruska (Prentice-Hall, 1990) is a good introduction. Other works of interest are *Building a Secure Computer System*, by Morrie Gasser (Van Nostrand Reinhold, 1988), and *Computer Viruses, Worms, Data Diddlers, Killer Programs and Other Threats to Your System: What they are, how they work, and how to defend your PC or mainframe*, by John McAfee and Colin Haynes (St. Martin's Press, 1989). The June 1989 issue of *Communications of the ACM* was devoted exclusively to the Internet worm.

For information on IBM's Antivirus Service Program, contact IBM Corp., 40-F2-01, 1 East Kirkwood Blvd., Roanoke, Texas 76299; 800-742-2493. One vendor of popular antiviral software is EME Enterprises, 4313 Highway 17 South, Department 208, Orange Park, Fla. 32073-7875 (904-269-7547), which sells F-Prot by Fridrik Skulason. Another is McAfee Associates, 3350 Scott Blvd., Building 14, Santa Clara, Calif. 95054 (408-988-3832), whose antiviral product is called Viruscan.

NETWORKS. The Computer Emergency Response Team at the Software Engineering Institute of Carnegie Mellon University, Pittsburgh, has a number of complimentary services and resources, including advisories on security vulnerabilities, and other articles and documents. Its 24-hour hotline is 412-268-7090. Internet e-mail address is cert@cert.org.

Sponsored by the U.S. Defense Advanced Research Projects Agency, Privacy-enhanced Electronic Mail (PEM) will be available to qualifying Internet organizations on Sept. 30. (U.S. export restrictions on cryptography apply.) For more information, write Trusted Information Systems Inc., Attn. PEM, 3060 Washington Rd. (Route 97), Glenwood, Md. 21738; 410-442-1673. The internet address is pem-info@tis.com.

CRYPTOGRAPHY. An excellent overview of public-key cryptography, by Bruce Schneier, appears in the May 1992 issue of *Dr. Dobb's Journal*.

Among several *IEEE Transactions on Information Theory,* classics are "New Directions in Cryptography, Vol. IT-22, no. 6, pp. 644–54 (November 1976) by Whitfield Diffie and Martin E. Hellman, which put forth public-key cryptography, and "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm," Vol. IT-31, no. 4, pp. 473–81 (July 1985) by Taher ElGamal, which influenced the proposed Digital Signature Standard. The *Communications of the ACM*, Vol. 21, no. 2 (February 1978) is where R.L. Rivest, A. Shamir, and L. Adleman published the RSA method of public key encryption in "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," pp. 120–26. "The First Ten Years of Public-Key Cryptography" by Diffie appeared in the May 1988 *Proceedings of the IEEE*.

The Second CPSR Cryptography and Privacy Conference, June 1, 1992, by the Computer Professionals for Social Responsibility, Washington, D.C. (202-544-9240) has a thick resource book (out of print). A third conference is being planned for June in the coming year.

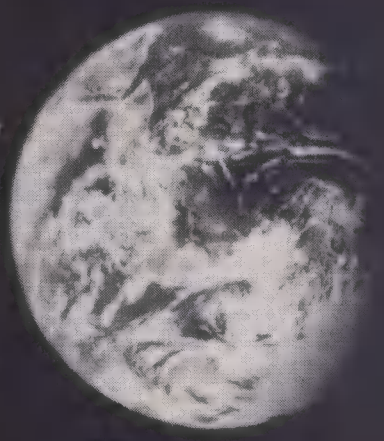
The U.S. National Institute of Standards and Technology will be publishing its revised version of the proposed Digital Signature Standard this month. A periodic public review of the Digital Encryption Standard begins in January.

IEEE conference proceedings take you to the frontier in electronics and computing...

...and our Prepaid Order Plan gets you there at a savings of about $5,000!

The 1992 IEEE Prepaid Order Plan (POP)

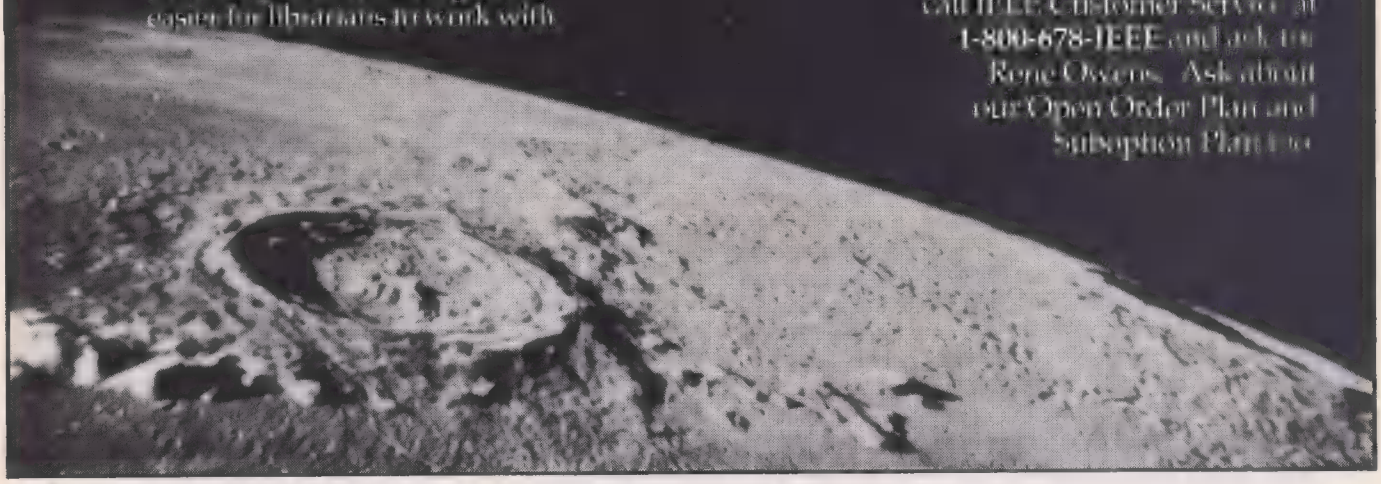
If your library needs leading edge information in computing and electronics first, fast, and at a reasonable price, consider IEEE conference proceedings. Plus, with our Prepaid Order Plan, your library can get these important proceedings -and save about $5,000!



Our Prepaid Order Plan brings you these major benefits:

- **Save about $5,000**
  Pay only $8,995 for the 1992 Plan – that's about $5,000 off the combined proceedings prices!
- **Free 1992 Index**
  You'll get the new 1992 two-volume *Index to IEEE Publications* – a value of about $350 – *free*
- **Get key work first**
  IEEE conference proceedings publish innovative research first – *before* journals, magazines, books, on-line services, CD-ROM or any other media
- **Now with ISBNs**
  IEEE conference proceedings now carry ISBNs, making them easier for librarians to work with

To order, or for a free brochure, call IEEE Customer Service at **1-800-678-IEEE** and ask for Rene Owens. Ask about our Open Order Plan and Subscription Plan, too.



MIL reliability: a new approach

Traditionally faulted for not predicting reliability accurately, MIL-HDBK-217 now has an alternative waiting in the wings

Feelings run high about MIL-HDBK-217. Otherwise known as the "Reliability Prediction of Electronic Equipment" Handbook, it has been the focus of a battle of words in the reliability engineering journals of the last few years. Even at reliability conferences, heated, sometimes acrimonious, arguments break out among normally dignified and restrained engineers when the subject of the handbook is broached.

At issue is the handbook itself. Is it worthless or worse? Or is it a helpful and necessary standard guide—albeit misunderstood and much maligned one?

Opponents of MIL-HDBK-217 say that it is inaccurate, leads to costly overdesign, actually prevents higher reliability levels from being achieved, and does not address the true causes of failures. Moreover, they say, the handbook's models are out of date and do not reflect emerging technologies.

Adherents defend MIL-HDBK-217 as a necessary standardized medium for assessing reliability and comparing designs. They maintain that it is based on careful analysis of part and system reliability data. Any problems arising with the handbook, they say, are caused by misinterpretation or misuse of it.

Controversial as it is, the handbook has long been the U.S. Department of Defense's (DOD's) bible for predicting reliability. But it may soon be supplanted, at least as it pertains to integrated circuits. Recently, the U.S. Army Material Command, Aberdeen Proving Ground, Md., proposed development of a new handbook based on analytical physics of failure; the current handbook is based on empirical statistical observations.

MIL-HDBK-217 got its start in the early 1960s as the new discipline of reliability engineering grew. The handbook was developed under the auspices of the U.S. Air Force's Rome Air Development Center, now the Rome Laboratory, at Griffiss Air Force Base, Rome, N.Y., and quickly became the most widely applied reliability prediction tool.

Over the years, it has gone through many revisions, the latest being 217F, issued Dec. 2, 1991. In that version, the handbook's stated aim is "to establish and maintain consistent and uniform methods for estimating the inherent reliability (i.e., the reliability of a mature design) of military electronic equipment and systems."

Contractors to the U.S. Department of Defense, Washington, D.C., are explicitly required to use the handbook to estimate the reliability of their products; those estimates are then compared to the reliability specifications called for, as well as to the reliability of competing designs. Producers of nonmilitary electronic equipment, such as instruments and avionics gear, also often elect to adhere to the handbook—even though they are not expressly required to do so—because it offers a convenient and standard way of estimating reliability.

MIL-HDBK-217 covers microcircuits, including silicon gate arrays, microprocessors, and memories, and gallium arsenide ICs; discrete diodes and transistors; lasers; and such fundamental components as resistors, capacitors, relays, and connectors. For each of these areas, the handbook presents a straightforward equation for calculating the failure rate in failures per million hours.

> A constant failure rate may have been valid for vacuum tubes, but solid-state components' failure rate may approach zero

For a CMOS gate array, for example, the equation includes terms and factors representing the number of gates on the chip, the junction temperature, the package type, the environment, the years the generic device type has been in production, and the quality control the chip has been subjected to. To calculate the overall failure rate, an equipment designer simply adds the failure rates for all components in a system.

For implementing the handbook, a software program, Oracle, is available from the U.S. Air Force's Rome Laboratory. Several proprietary programs are also available, and even some electronic design automation systems that implement MIL-HDBK-217 routines.

LIMITED OPTIONS. To bring the estimated reliability into line with the required reliability, the designer varies the factors—that is, changes the selection of components or alters the operating conditions. But a problem with the handbook, critics say, is that options for improving the calculation are limited; usually lowering the junction temperature and choosing hermetically sealed packages are resorted to because they have the biggest effect under handbook rules.

Today the handbook is used in developing the Comanche light helicopter, the advanced tactical fighter, the B2 bomber, and most other military projects. It is also used in the Boeing 777 commercial airplane and has been adopted by the Underwriters Laboratories, Northbrook, Ill., as UL-991 for use with commercial electronics equipment.

The National Aeronautics and Space Administration (NASA), Washington, D.C., also uses MIL-HDBK-217 for probabilistic analyses. Recently, the handbook was applied to a reliability analysis of NASA's space station. "It's a useful document," Joseph Fragola told *IEEE Spectrum*. Fragola is vice president of the Advanced Technology Division of Science Applications International Corp. (SAIC), New York City, which serves as a reliability consultant for NASA. "We use it all the time with NPRD-5 ["Non-Electronic Parts Reliability Data," from the Rome Laboratory], which is a broad-based software package, and program-specific and type-specific data," he said.

NASA's Jet Propulsion Laboratory, Pasadena, Calif., and Goddard Space Flight Center, Greenbelt, Md., are particularly dependent on the handbook as a "starting point," Fragola said, because of their work on robotics and electronics for long-term service. "For the space station, NASA was forced to use probabilistic analysis and quantitative numbers because they had to come up with an estimate of what the maintenance load would be over 40 years. There's no way to do that except by having reasonable failure rates based on the information in documents like 217."

As to timeliness, Fragola noted, "One of the problems with 217, and everybody knows

George F. Watson Senior Editor

0018-9235/92/$3.00©1992 IEEE

this, is that electronics technology is extremely volatile, and information tends to get stale rapidly. That necessitates updates on a regular basis, and it's not cheap."

AVOIDING RESPONSIBILITY. But acceptance of MIL-HDBK-217 is often grudging. An outspoken critic of the handbook, Charles Leonard, who develops packaging technology at the Boeing Commercial Airplane Group, Seattle, Wash., told *Spectrum*, "The commercial avionics industry isn't bound to abide by 217. But when faced with the necessity for a reliability prediction and with 217 listed as an acceptable methodology, suppliers have little choice. Some people feel it has other benefits as well. I've had box design engineers say to me, 'It's a valuable tool. It allows me to turn over the reliability issues to the reliability group and we box designers don't have to be concerned any more. They run the numbers and we do our work.' "

That is an abrogation of responsibility, in Leonard's view. "We have used the concepts of MIL-HDBK-217 to guide engineering and management decisions and in so doing have incurred large costs and deflected attention from reliability-enhancing measures that could be more effective," he said. Leonard favors applying the physics of failure directly to product development instead of relying on the handbook to estimate reliability. He advocates what he calls a stress-margin approach [Fig. 1].

Equally outspoken is Patrick D. T. O'Connor, reliability manager at British Aerospace Dynamics, Stevenage, United Kingdom. "I think the only balanced view is to say that MIL-HDBK-217 and anything like it is the biggest load of garbage ever to be foisted by engineers on other engineers and should immediately be done away with," he told *Spectrum*.

In the United Kingdom, the Ministry of Defense, London, has issued new guidelines on reliability prediction in which parts-level methods required by the handbook are relegated to "nonpreferred" status. French and German contractors tend to follow MIL-HDBK-217 on military projects, O'Connor said, but he has found that many Japanese companies are skeptical of using the method.

Meanwhile, work is proceeding in Europe on alternatives to 217. The International Electrotechnical Commission, Geneva, Switzerland, is developing standards for reference conditions for reliability prediction and for screening through its Technical Committee 56, for example. The International Organization for Standardization, also in Geneva, has prepared a standard for assessing the competence of component manufacturers. Now circulating for comment, the standard would be used to help system developers build confidence in suppliers' reliability practices, so that system reliability predictions can be based on vendor- and component-specific data rather than on averages.

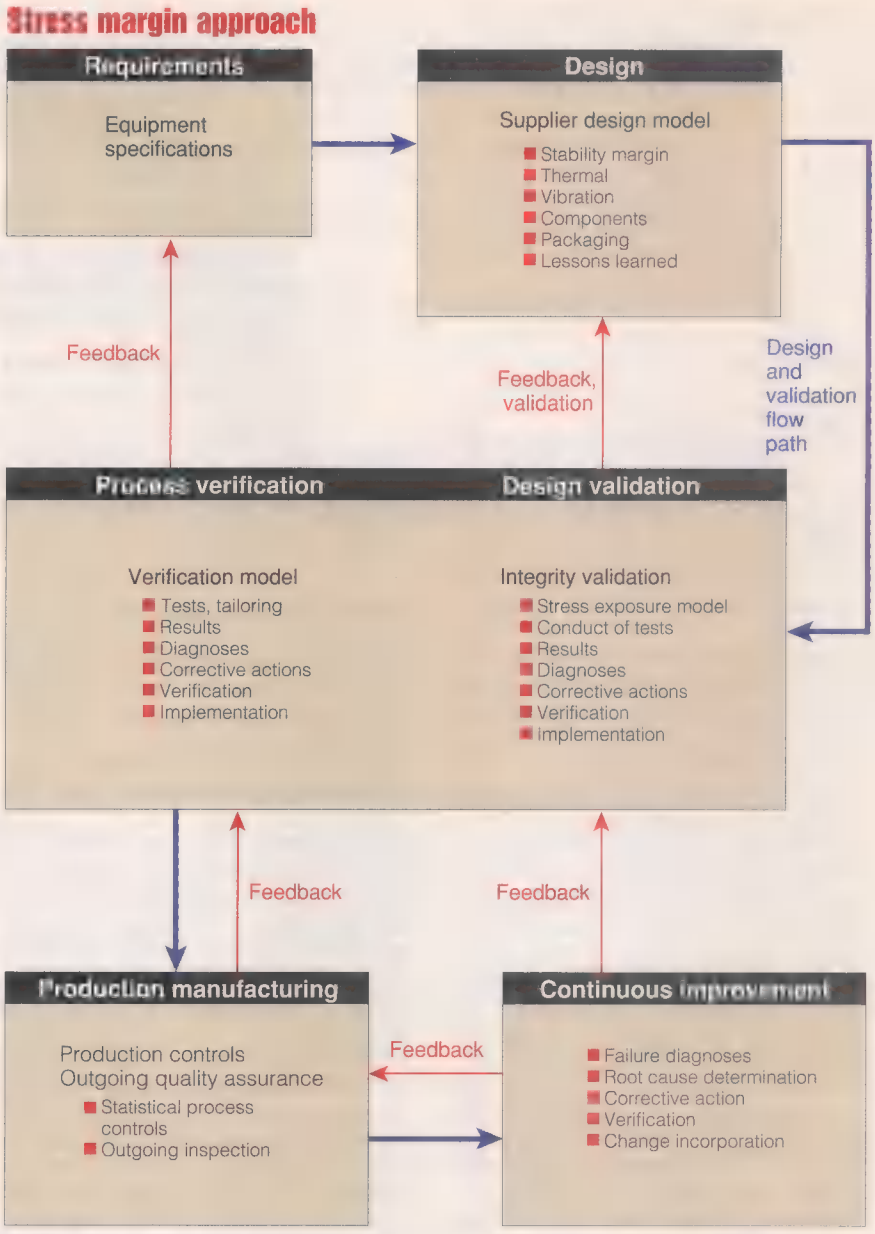
Although the best-known handbook of its type, MIL-HDBK-217 is not the only one. Bellcore, British Telecom, and Nippon Telephone and Telegraph, for example, have produced handbooks based, like MIL-HDBK-217, on failure prediction methodology (FPM). That process produces empirical values for failure tendencies such as mean time between failures or failure rate per unit of operation. However, the various FPM guides yield widely different predictions.

A major complaint of handbook critics is that it assumes a constant rate of failure over the useful life of components, ranging from ICs to solder joints—the familiar bathtub curve [Fig. 2]. That is, between an initial period of infant mortality and a final wear-out period, failures are assumed to occur at a constant rate that can be minimized by choosing higher-quality components (usually, those that have had more screening) and by reducing thermal and electrical stress.

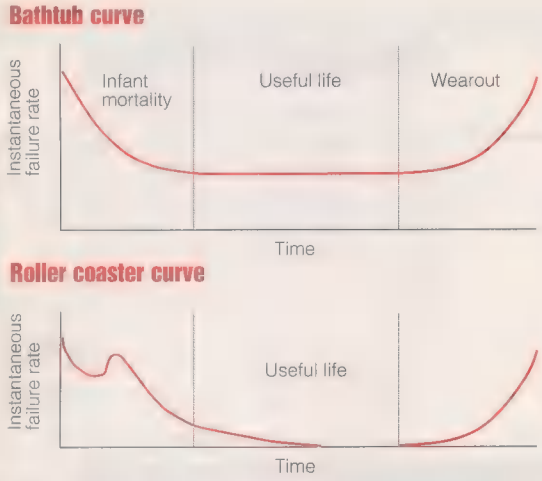
The assumption of constant failure rate may have been valid in the days of vacuum tubes, critics say. But, for solid-state components, many contend, failure rate decreases, perhaps even approaching zero.

Indeed, the cause of failure is often not a defect in the component but a result of human errors—like subjecting the component to electrostatic discharge damage, choosing the wrong component for an application, or misinterpreting the component's specifications.

Many reliability experts take issue with this complaint, however. "Such a view is a rather limited perspective of what a failure rate is," SAIC's Fragola told us. "More properly, all causes of failure *should* be included, since the equipment doesn't discriminate between causes. When all causes are considered, the recorded constant fail-



[1] Boeing Co. and the Electronic Packaging Center at the University of Maryland are developing a method of product development that uses continual feedback to improve reliability.



[2] Instead of the constant failure rate represented by a bathtub curve, a curve representing a decreasing failure rate during useful life may now be appropriate.

ure rate may well represent actual in-field performance."

Though defective components have caused failures, the quality standards of most modern components are so high that usually only a few per million are defective in ways that could lead to failure in use.

Another fundamental objection to the handbook is its assumption of an Arrhenius relation—that the tendency of an electronic component to fail increases exponentially with its temperature. On the basis of this assumption, MIL-HDBK-217 includes a temperature multiplier [Fig. 3] for failure rate calculations. The multiplier is determined by measuring failure rates of devices at high temperature and extrapolating the measurements to normal operating temperature.

The extrapolation depends on the value selected for the acceleration factor, and, critics say, the values used are averages and are not directly related to specific failure mechanisms. In addition, they say, high-temperature testing induces wearout failure mechanisms that do not occur at normal temperatures.

SMALL BUDGET. The handbook is administered by a small group of engineers at the Rome Laboratory who oversee a relatively small budget. "Many people think that millions of dollars and many worker-years are spent on maintaining the handbook," Seymour F. Morris, program manager for MIL-HDBK-217 at the laboratory, told *Spectrum*. "Unfortunately, that's not the case, and with the cuts in DOD funding, the situation will probably get worse."

For the past 20 years, the Rome Laboratory has expended 1–1.5 worker-years per year on maintaining the handbook, and has allocated about US $200 000 per year to outside contractors for studies to update sections of the handbook. A typical study costs $150 000–$200 000, an amount that limits the laboratory to only one new start a year.

Mindful of criticism of the handbook, Morris told us, "Adverse comments are often the result of misconstruing when and how the handbook should be interpreted." He maintained that MIL-HDBK-217 is intended to provide a consistent and uniform database for making reliability predictions when specific experience data does not exist. Before the handbook became available, each military contractor would have its own set of reliability data and comparisons among contractors were difficult or impossible.

"MIL-HDBK-217 isn't intended to predict field reliability and generally doesn't do a good job of it," Morris said. "But this doesn't diminish its value, since achieving its purpose doesn't require an absolute prediction of field reliability." The handbook should be thought of as a leading indicator that gives a relative measure of expected reliability. Morris likens it to such indicators as gas mileage ratings for cars, weather forecasts, and economic indicators that, used properly, give valuable insight into the kind of future to expect.

Problems with the handbook are often introduced by users themselves when they apply it blindly, NASA consultant Fragola contends. "If you're careful and you use it wisely, not as an answer but as an input, it's fair to say that it's a valuable tool," he said.

GETTING OPINIONS. Anthony J. Feduccia, chief of the Systems Reliability and Engineering Division at the Rome Laboratory, told us that opinions on MIL-HDBK-217 are continually solicited from industry and military agencies. For the most recent version, 217F, the laboratory mailed draft copies to government agencies, companies, industry associations, and professional societies. An additional 200 copies went to individual requesters after the first mailing. Over 250 comments were received from about 25 organizations, including some of the handbook's harshest critics. The Rome Laboratory is not bound to accept comments, of course, but it usually provides an explanation for not doing so.

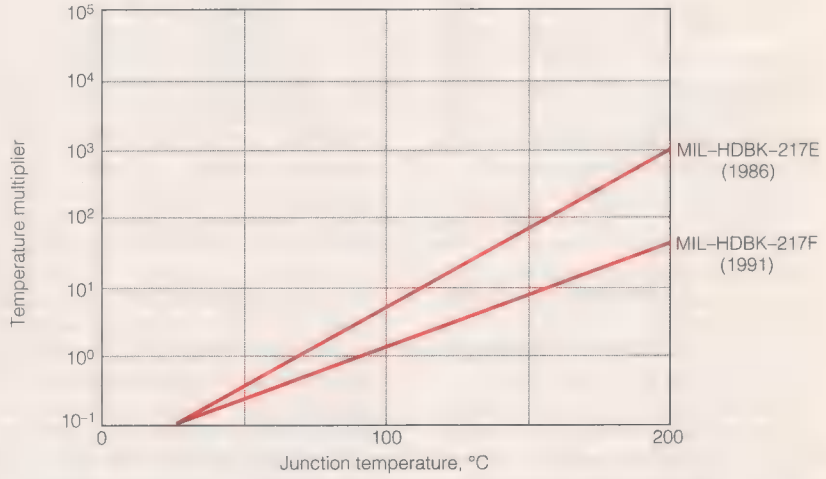
"The handbook's critics fail to realize that reliability prediction is only a part of an overall reliability program," Feduccia said. "A prediction based on the handbook is an estimate of the inherent reliability of a design based on historical data and should be interpreted as such. There is no statistical confidence level associated with the prediction, and the calculated mean time between failures should not be blindly compared to operational reliability. The prediction is simply a design tool for comparing design options, identifying overstressed parts, and providing input for analyses."

Feduccia challenges detractors to suggest an alternative to MIL-HDBK-217. "What do we put in its place?," he asked. "Is the alternative to let contractors do whatever they want to do, with no government intervention at all? Personally, I'm not ready to subscribe to that philosophy."

The handbook's database derives largely from about 35 technical reports published by the Rome Laboratory. Most reports have been generated by 12–18-month contractor studies that investigate the reliability of specific component types.

The most recent study was done for the 1991 version of the handbook, 217F. IIT Research Institute, Chicago, and Honeywell Solid State Electronic Systems Division (SSED), Colorado Springs, Colo., collaborated to propose new reliability models for CMOS very high-speed ICs (VHSICs), and Westinghouse Electric Corp., Pittsburgh, and the University of Maryland in College Park joined forces to propose models for high-gate-count ICs and for chips in complex packages such as surface-mount, application-specific ICs (ASICs), and hybrid devices.

Michael Pecht, a researcher who led the University of Maryland's part of the study at the Calce Electronic Packaging Research Center there, told us that it became clear



[3] The multiplier for the temperature term in the handbook's failure rate equation increases exponentially. The plots are for hermetic-package CMOS ICs.

to the contract researchers that the Arrhenius relation in the device was inappropriate, and recommended to the Rome Laboratory that it not be included in the new edition. "Both the IIT/Honeywell and Maryland/Westinghouse teams noted that temperature cycling is more harmful than operating a device at a steady high temperature as long as it is below a critical value," Pecht said.

The recommendation was not accepted, however. "The approach was unusable by our audience," Rome's Feduccia said. "We have to gear the handbook to a specific audience: reliability analysts on both the government and contractor sides. It would take a Ph.D. to use the models, and they needed a lot of advance information that most people don't have."

Yet, uncompromising adherence to the Arrhenius relation causes overdesign and may be dysfunctional, Boeing's Leonard claims. "Simply reducing temperature can boost cost and weight without compensating benefit," Leonard said. "Temperature reduction can mean extra weight, volume, and power consumption, and in an airplane, such penalties must be justified. They reduce the payload and the range, and the additional complexity can reduce reliability. The need for temperature reduction should be clearly justified, and it should be done only after the options have been exhausted."

According to Leonard, another example of the handbook's tendency to increase costs without identifiable benefits is its "bias toward MIL SPEC-screened ceramic parts, by virtue of its quality factor term in the equations. The large difference in predictive factors essentially precludes consideration of modern plastic-encapsulated parts that can be more reliable than more costly ceramic-packaged chips in many military and aerospace applications."

That the handbook favors quality-control screening also draws Leonard's fire. "The need for screening should be viewed as an indicator that the manufacturer needs to pay attention to its processes and controls and eliminate the causes of failure that screening attempts to weed out," he told us.

MARGINS OF STRESS. As an alternative to the handbook, Leonard has proposed the stress-margin approach to design, development, and product validation. With the University of Maryland's Electronic Packaging Research Center, Boeing is developing the approach for possible adoption. Product development would flow from establishing equipment specifications through design, qualification testing, manufacturing process verification, and postdelivery improvement, with feedback on product quality and reliability at every step [Fig. 1]. It is the lack of failure diagnosis, analysis, and feedback that Leonard says is the basic flaw in the MIL-HDBK-217 approach.

The first step in stress-margin–based product development is to design a product by using models based on physics-of-failure analyses. Next, the product is exposed to highly accelerated stresses to uncover weaknesses that otherwise would result in failures. The failures are diagnosed for their root causes and corrections are decided on, validated, and fed back into the design models for future use. "It is a never-ending process that continually modernizes the design model," Leonard said.

MAJOR BOOST. The physics-of-failure approach received a big boost in June when the U.S. Army Materiel Command authorized a $1 million program to institute a transition from reliance exclusively on MIL-HDBK-217. The command's Army Materiel Systems Analysis Activity (Amsaa), Communications-Electronics Command (Cecom), and Laboratory Command (Labcom) and the University of Maryland's Calce group will collaborate on developing a physics-of-failure handbook for reliability assurance. The handbook will present a methodology for assessing system reliability on the basis of environmental and operating stresses, the materials used, and the packaging selected. Physics-of-failure software will also be developed.

> The Defense Department is encouraging the Navy and Air Force, as well as the Army, to adopt physics of failure

"We're aiming to have the handbook ready in 12 months," Edward B. Hakim, chief of the Reliability, Testability, and Quality Assurance Branch at Labcom's Electronics and Technology Devices Laboratory, Fort Monmouth, N.J., told *Spectrum*. "A lot of the work has already been done by Calce." After the handbook is released, it will be coordinated with the software tools, which will be tested at sites at the DOD, at various universities, and at several companies.

The Rome Laboratory's Feduccia, however, questions whether a physics-of-failure handbook can be readied so quickly. "The proposed handbook should go through the same coordination process and the same scrutiny that 217 goes through," he said.

Hakim, of Labcom, has found widespread interest at the DOD in the physics-of-failure approach. The department is encouraging the Navy and the Air Force, as well as the Army, to consider the method. "The Navy is very interested in participating," Hakim said. "It seems that they will actively support the beta site effort."

Hakim stressed that the new handbook will not be a direct replacement for MIL-HDBK-217. "I don't want people to think we're producing another handbook that has models you can plug numbers into to get a reliability prediction," he said. "It will be more like guidelines. It's going to be very generic. The main result of the effort will be the software tools we develop."

The Air Force Systems Command, Wright-Patterson Air Force Base, Ohio, is also exploring physics-of-failure reliability models. The Systems Command funded a study of a comprehensive reliability prediction model based on the premise that essentially all failures are caused by interaction of built-in flaws, failure mechanisms, and stresses.

Will a physics-of-failure approach lengthen the lead time for product development? The University of Maryland's Pecht thinks not. "It will demand a little more expertise in upfront design," he said. "But it will greatly reduce screening and testing requirements. And it's going to dramatically reduce rework."

These are major reasons for the Army's interest, Pecht said. "In the new generation of military products, there may be very few built, maybe only a prototype," he told us. "The Army wants to be sure it works the first time."

REWRITING A STANDARD. A key goal of the Army Materiel Command is to rewrite MIL-STD-785, "Reliability Program for Systems and Equipment Development and Production." This standard is the fundamental specification in the hierarchy of reliability specifications and requires that MIL-HDBK-217 be used for reliability prediction and modeling. This results in the handbook being used in reliability testing, screening, device selection, derating, maintainability analyses, and logistics analyses.

"We want to remove the influence that MIL-HDBK-217 has on MIL-STD-785 and integrate the physics of failure approach into it," Hakim said. A new draft standard will be prepared while the new handbook is readied. Even more ambitiously, proponents hope eventually to integrate a physics-of-failure standard into a nationally—and perhaps internationally—accepted industrial standard.

TO PROBE FURTHER. MIL-HDBK-217F, "Reliability Prediction of Electronic Equipment," is available from the Standardization Document Order Desk, 700 Robins Ave., Building 4, Section D, Philadelphia, Pa. 19111-5094; 215-697-2667.

The *IEEE Transactions on Reliability* frequently publishes papers on reliability prediction and physics of failure. See, for example, in the March 1992 issue, "A Survey of Reliability Prediction Procedures for Microelectronic Devices" by J. B. Bowles.

The International Reliability Physics Symposium will next be held on March 22–25, 1993, in Atlanta, Ga. For general conference information, contact David Baglee, Intel Corp., MS F9-99, 4100 Sara Rd., Rio Rancho, N.M. 87124

Cooperating on superconductivity

AT&T, IBM, and MIT have been working together on superconducting electronics, and here's what they have accomplished so far

In the late 1980s, there were fears that the United States would fall behind in the development and commercialization of high-temperature superconductivity. So on March 15, 1988, a committee was formed by the President's Council of Advisors on Science and Technology to advise the executive branch on how to improve the country's competitive position in this field. Ralph E. Gomory, then chief scientist at IBM Corp., was named to the chair of the committee, which within a year produced several recommendations.

An immediate consequence was the formation of the Consortium for Superconducting Electronics (CSE) by IBM, AT&T, the Massachusetts Institute of Technology (MIT), and the Lincoln Laboratory, which is run for the Federal government by MIT. The organization has now been in existence for approximately two years—long enough not only to have formulated goals and methods but to have achievements to report as well.

The Gomory committee had judged that it would take a decade or more to bring high-temperature superconductivity to market, and only broadly based consortia would have the resources and stability to persevere to a successful conclusion. So in a key recommendation, the committee had urged that precompetitive R&D in the technology be conducted by a number of consortia linking universities, government laboratories, and industrial laboratories.

The committee's report was released in January 1989, and the four future members of the CSE began negotiations in the same month. By October 1989, negotiations were complete and a proposal had been sent to the Defense Advanced Research Projects Agency (Darpa), Arlington, Va., for funding of the university and government laboratory parts of the consortium. Research began as soon as the participation agreement binding the members to the CSE had been signed.

Richard W. Ralston MIT Lincoln Laboratory
Marc A. Kastner Massachusetts Institute of Technology (MIT)
William J. Gallagher IBM Research Division
Bertram Batlogg AT&T Bell Laboratories

SIMPLIFIED MANAGEMENT. Managing a research program involving four large institutions is a far from trivial task. Nevertheless, it has proved possible to accomplish with a rather simple organizational structure [Fig. 1]. Primary authority for the consortium rests in the executive committee, which is chaired by the provost of MIT, Cambridge, Mass., and has one representative from each of the founding institutions.

Below the executive committee is a four-person directorate, which carries out the day-to-day management of the CSE. It comprises one director from each of the four institutions, with Richard W. Ralston of the MIT Lincoln Laboratory, Lexington, Mass., as principal director. The directorate makes recommendations to the executive committee about the expenditure of funds, new members, and the more important new programs.

So far, the CSE has undertaken four major programs: in materials and processing, junctions, networks, and circuits. The managers of those programs advise the directorate about the addition or termination of projects. Although the managers are each affiliated with one member institution, the activities of the individual programs cross institutional boundaries.

> Only a consortium would persevere until high-temperature superconductivity reached the market

Early in the life of the CSE, the group realized that specific goals would have to be set if the consortium's efforts were to be successful. Such goals were therefore established in the Darpa proposal for each year of funding for each of the programs [see table, p. 54]. The table also summarizes the progress made in each of the four program areas toward meeting those goals during the consortium's first year.

A key element that helped in realizing those successes was that, at the time the consortium was founded, the member institutions had substantial "base" activities in the area of thin-film superconductors. They believed it would be expedient to pool the base efforts and achievements—in hardware, learning, intellectual property, processing art, and so on—and combine that work with the work made possible by the Darpa funding.

Thus, current CSE programs are a combination of base activities (some funded by Government agencies) and new initiatives.

MATERIALS AND PROCESSING. Since the CSE is concerned with electronic (as opposed to large-current) applications of superconductors, it deals with superconductors mainly in the form of thin films. Of primary importance, then, especially in these early years, is the CSE's materials and processing program, which develops and evaluates substrate materials and film-deposition techniques for specific applications.

Because factors like critical temperature (T_c), crystallographic orientation, critical current density (J_c), surface smoothness, surface resistance, and large-area homogeneity have different relative importance for different applications, no single criterion can be used to judge the quality of a superconducting film. Nevertheless, the CSE did set several overall goals for the first year of the program.

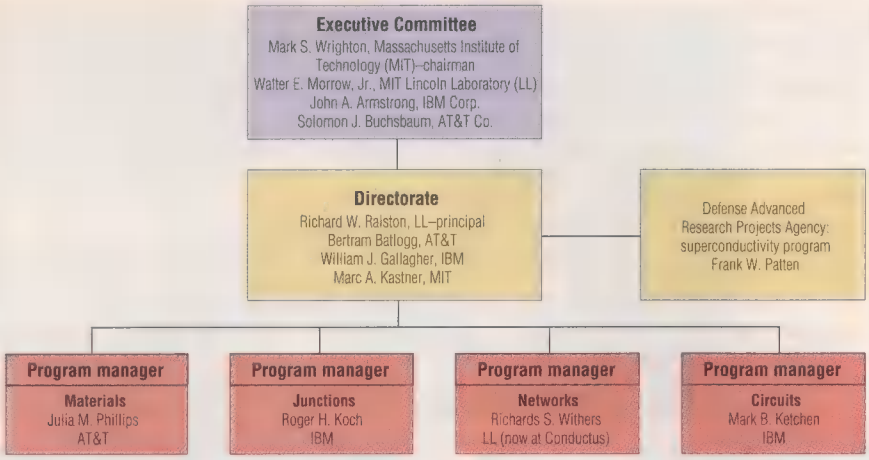
Members agreed it was clearly necessary for all applications to develop large-area substrates, to prepare films of all types with high critical current densities, and to learn how to fabricate multilevel structures

SUBSTRATE GOALS. The strong base program AT&T Bell Laboratories, Murray Hill and Holmdel, N.J., had achieved in crystal growth allowed the CSE's early goals for substrates to be met quickly—no small achievement given the stringent requirements that substrates for superconducting films must meet.

For example, since most high-temperature superconductors are based on copper oxides, the substrates must be able to withstand the high temperatures (around 700 °C) associated with cuprate deposition.

It is also crucial that the lattice constant and coefficient of thermal expansion of the substrate be closely matched to those of the film. Furthermore, all high-frequency appli-

0018-9235/92/$3.00©1992 IEEE



[1] This simple management structure has proven adequate for coordinating the efforts of four large institutions. Each program involves researchers at several member organizations.

[2] Boules and wafers of orange $LaAlO_3$ and dark $NdGaO_3$ with diameters of 25, 50, and even 75 mm (for $LaAlO_3$) are now being produced regularly by the consortium.

cations require substrates with low loss, and some require a low dielectric constant as well.

After ▪ first round of evaluation, researchers found that neodymium gallate ($NdGaO_3$) and lanthanum aluminate ($LaAlO_3$) appeared to be good candidates for many applications. Large crystals (about 50 mm in diameter) of those materials are now grown routinely at AT&T by the traditional Czochralski technique using iridium crucibles [Fig. 2].

THIN-FILM DEPOSITION. Because it is still not clear how to make the best film for any specific application, the consortium is intensifying efforts to optimize a variety of deposition techniques, including sputtering, coevaporation, laser ablation, and molecular-beam epitaxy. In comparing these various deposition methods, results like phase purity, surface smoothness, and electrical performance must be considered along with such production aspects as deposition rate and processing ease.

All the techniques are now routinely producing the workhorse superconducting material known as YBCO ($YBa_2Cu_3O_x$ and pronounced "yibcoe"). With each CSE member concentrating on the deposition method it does best, overall YBCO film processing is maturing at a rapid rate.

Since several problems are common to all the deposition techniques, they are being studied extensively. For example, joint efforts are under way to design substrate heaters and to identify the optimal gas composition for the *in situ* annealing of YBCO and other cuprate films such as TlBaCaCuO (TBCCO) and BiSrCaCuO (BSCCO).

For microwave filters, high-quality YBCO films have been deposited on both sides of large-diameter (50-mm) lanthanum aluminate substrates with acceptably low dielectric constant and loss. The films were made using the so-called barium fluoride process, which involves vacuum coevaporation of yttrium, copper, and barium fluoride (BaF_2), followed by *ex-situ* annealing.

Another method for fabricating thin YBCO films was developed in a base program funded by Darpa at MIT. In the organometallic deposition technique, trifluoroacetates are sprayed onto the substrate and then fired in air to burn away the organic materials. The method has yielded critical temperatures above 90 K and critical current densities of about ▪ million amperes per square centimeter at 77 K.

The process is of interest because of its simplicity and its potential for scaling to large-area coverage. Before it can be used for interconnect and filter applications, though, it will have to be refined to eliminate voids and improve surface smoothness.

A potentially interesting alternative to the cuprates, despite its modest T_c of 30 K, is ▪ high-temperature superconductor called BKBO (for $[Ba,K]BiO_3$). It has two advantages over the cuprates: its significantly

Defining terms

Annealing: the process of holding ▪ material at an elevated temperature for a specified length of time to induce structural or electrical changes in its properties.

Co-evaporation: ▪ process used for film formation wherein two or more materials are simultaneously evaporated onto ▪ substrate.

Critical current density (J_c): the maximum current density a film will carry as a supercurrent—that is, with zero resistance. It is a function of temperature and magnetic field strength.

Critical temperature (T_c): the maximum temperature at which a material is superconducting.

Ex-situ: processes of film formation in which a material is deposited onto a substrate maintained at ▪ temperature below the material's crystallization temperature. The film is crystallized in a subsequent annealing procedure.

Gradiometer, magnetic: a magnetic sensing device configured with two or more opposed sensing coils; it displays no sensitivity to uniform magnetic fields, but is sensitive to certain magnetic-field gradients.

In-situ: processes of film formation in which a material is deposited onto a substrate maintained above the material's crystallization temperature.

Josephson junction: two superconductors weakly coupled so that superconducting (Cooper) pairs of electrons can tunnel between them.

Laser ablation: ▪ film-deposition process in which a laser is used to vaporize ▪ material, which subsequently condenses onto ▪ substrate. The laser is usually pulsed.

Lattice constant: the dimensions of the smallest cell that, by periodic repetition, can be used to represent a crystal structure.

Squid: a superconducting quantum interference device, it senses the magnetic field flux threading a superconducting loop that is interrupted by one or two weak links. It is the most sensitive known detector of magnetic energy.

Superconducting coherence length: characteristic dimension of a superconducting (Cooper) pair of electrons, typically 1 to 5 nm in high-T_c copper-oxide superconductors.

Weak link: ▪ general term used to describe any weak connection between two superconducting bodies that displays the Josephson effect. Common weak-link structures are narrow constrictions and tunnel junctions.

longer superconducting coherence length and the isotropy of its electronic properties. Those properties of the cubic material make it more promising than the cuprates for devices based on weak links and tunneling effects. BKBO was discovered in the AT&T Bell Labs base program.

THE JUNCTIONS CHALLENGE. The long-term goal of the junctions program is to develop the technology to fabricate devices based on tunneling between two superconductors—a great challenge with cuprates because of their anisotropy and short coherence lengths. Nevertheless, as the table shows, much progress has been made, especially with superconducting quantum interference devices (Squids).

IBM has a long tradition of research in advanced Squid sensors. Before the consortium was formed, the company had conducted major R&D on high-T_c Squids, partly funded by the Office of Naval Research, Washington, D.C. That effort became one of the base programs under the auspices of the CSE. Since then, the main thrust of the Squid project has been to create a dedicated multilevel fabrication capability.

Earlier Squid work was done using films made available occasionally by researchers whose main focus was on growing novel materials. That research mode allowed the demonstration of several prototype Squids at 77 K and also permitted the verification of a sandwiching approach for coupling Squids to superconducting flux-focusing structures. However, researchers agreed that, to make further progress and demonstrate performance that would be of commercial interest, a dedicated film-growth capability was clearly necessary.

Under the CSE umbrella, the first two kinds of Squid-related structures made with a new dedicated fabrication system for multilevel structures were edge junctions and multilevel coils [Fig. 3]. In keeping with an early strategic decision, all of the pattern definition for these structures was done with standard photolithographic techniques—in the long run, the most desirable way to go.

The edge junction structure in Fig. 3 [topmost drawing on the left] is an attempt to kill two birds with one stone. First, it uses high-T_c films grown in the orientation most favorable for high J_c (with the CuO planes parallel to the substrate). At the same time, it makes a weak connection between two YBCO films in the direction of maximum coherence length, which is also along the CuO planes. The weak connection is in the area where the two YBCO films are separated by a fluoride layer or, as shown, a layer of $PrBa_2Cu_3O_x$ (PBCO), a non-superconducting cuprate.

LIMITING CONSIDERATIONS. It is well established that the supercurrent-carrying capability of a high-T_c film is maximized when the films are grown with their CuO planes parallel to well-polished planar substrates. Whenever such films are used to form stepped structures like contacts and line crossings, the performance of the structure will be determined by the achievable current density perpendicular to the planes.

A good device for evaluating that performance is a superconducting pickup loop combined with a multilevel coil. (The coil is required to focus the flux from a fairly large area into a Squid, which must be made small to be sensitive.)

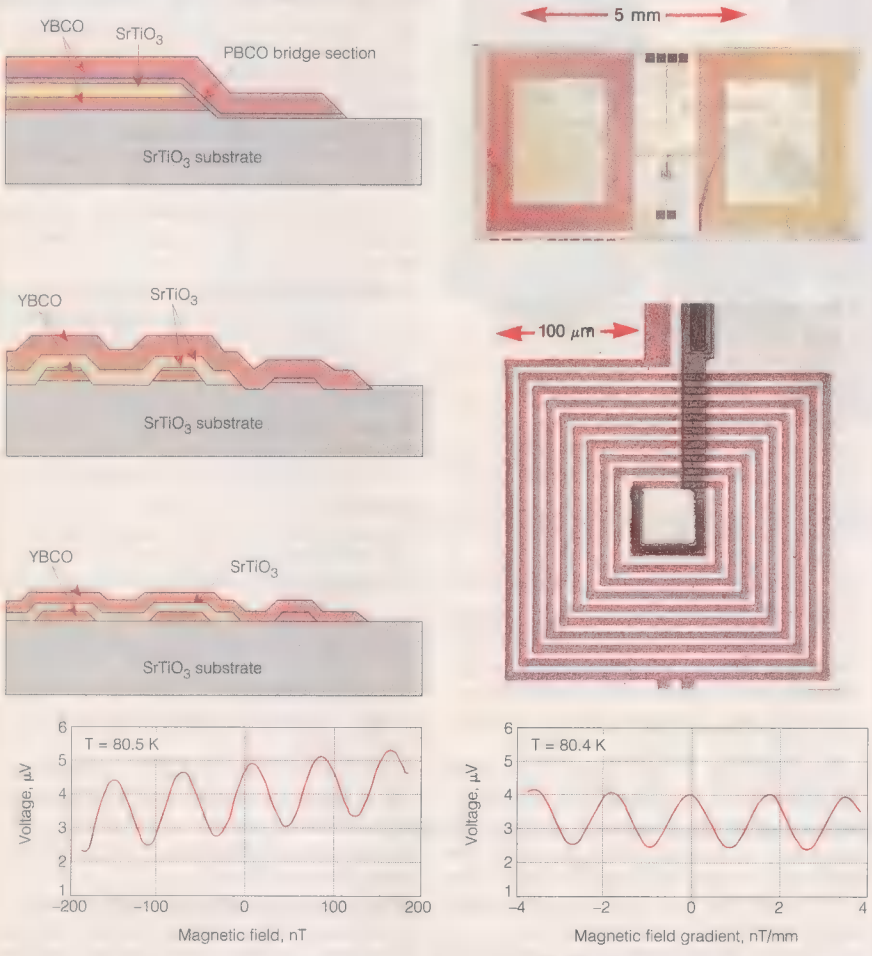
The ion-milled structure illustrated in Fig. 3 [middle drawing] was successfully used to make a 0.5-by-0.5-mm pickup loop connected to a five-turn coil. That coil, in turn, was coupled to a bicrystal Squid made on a separate substrate by pressing the two chips together. The resulting device was the first thin-film Squid magnetometer to operate at 77 K.

More recently, selective wet etchants have been used to build multilevel coil structures like the transformer shown schematically in the bottom drawing of Fig. 3. Selective wet etching is a more forgiving processing technique than ion milling; it has enabled the demonstration of a Squid gradiometer at 77 K [Fig. 3, photo]. Data on the uniform-field and gradient-field sensitivities of the gradiometer are presented in Fig. 3, at the bottom.

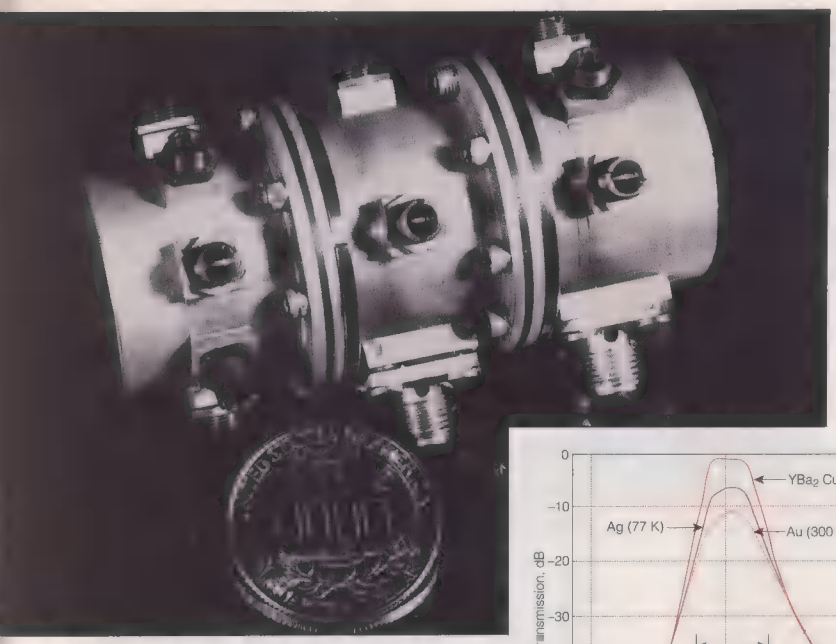
Other test results showed that the noise at 77 K for both the magnetometer and gradiometer came mostly from the Squids—white and inverse-frequency (1/f) noise—and not from the pickup coils.

MICROWAVE NETWORKS. The network program is directed toward microwave applications of high-temperature superconductors and toward using those superconductors to interconnect semiconductor devices. In the microwave area, a high-Q resonator has been constructed and delay lines and filters have been demonstrated—all using YBCO films.

Because of the very low microwave surface resistivity of superconducting thin films, compact filters made from them exhibit much lower losses than similar devices made with normal metals. Such compact filters were being worked on by Lincoln Laboratory under a base program funded by the Naval Research Laboratory, Washington, D.C., with the help of filter designers at Comsat Laboratories, Clarksburg, Md., which had considerable experience in filter



[3] The first Squid-related structures made with the new multilevel fabrication system include an edge junction structure, a portion of an ion-milled transformer, and a selective-wet-etched transformer [top, middle, and bottom drawings]. The system has been used to build a Squid gradiometer [photo above an enlargement of its 10-turn transformer]. The output voltage response for the gradiometer pick-up coil coupled to a Squid is shown as a function of a uniform field [bottom left] and a gradient field [bottom right].



[4] A superconductive filter has an enormous size advantage over a comparable cavity filter [photo]. The response curves compare the performance of the YBCO filter with similar filters made of silver and gold.

design for satellite communications.

Meanwhile, Bell Labs had developed a coevaporation technique for depositing YBCO films on both sides of large-area substrates like lanthanum aluminate.

With the formation of the CSE, the two efforts came together. Using a Comsat design developed specifically for the dielectric properties of lanthanum aluminate, Lincoln Laboratory developed techniques for patterning, contacting, and packaging filters produced with thin films deposited at Bell Labs.

The results were dramatic [Fig. 4]. At 4 GHz and 77 K, the YBCO filter had less than one-quarter the loss of ■ similar one made out of silver. That low loss translates to ■ Q of better than 1000 for each of the four resonant sections (the U-shaped structures) of the filter, which is what gives the superconducting filter its low insertion loss and steep skirts. Such performance is simply not possible with non-superconducting materials.

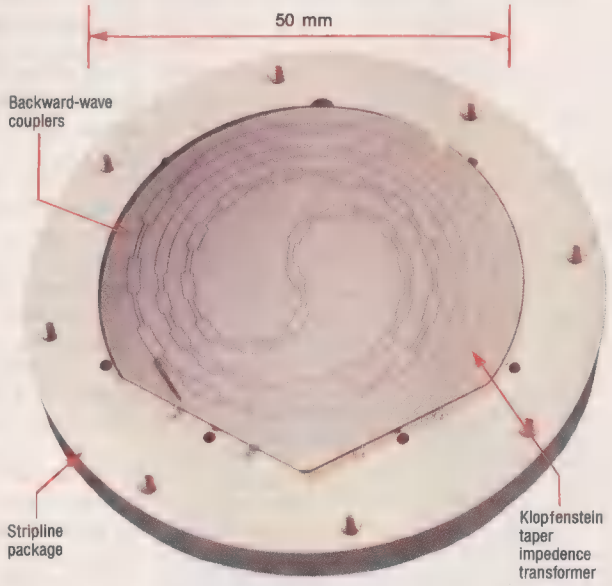
SIGNAL PROCESSING. Of equal importance to the construction of high-performance microstrip filters have been the thin-film quality improvements that have made practical power levels for receivers and signal-processing systems possible. Starting with sputtered thin films, Lincoln Laboratory has made filters capable of supporting 100 mW of transmitted microwave signal. Beyond that power level, nonlinearities caused by flux penetration of the superconductor distort the filter response.

Another important filter development that came about from cross-institutional collaboration was the fabrication of chirp filters, which are used to create radar pulses of very short duration. Such filters are ■ good example of the need to make high-performance transmission-line circuits on large substrates. Whereas typical bandpass filters for signal conditioning fit on ■ 10-by-10- or 10-by-20-mm substrate, ■ chirp filter requires ■ much larger area.

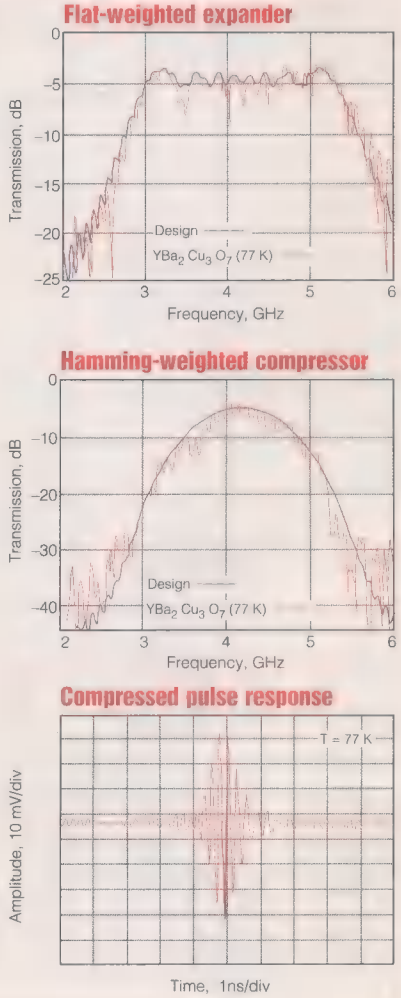
For example, Lincoln Laboratory needed 50-mm substrates coated with YBCO film to build such a filter. It obtained coated lanthanum aluminate substrates of the required size from AT&T and thus was able to build ■ chirp filter consisting of 48 backward-wave stripline couplers [Fig. 5]. The desired linear variation of time delay as a function of frequency, or chirp response, is obtained by having the length and spacing of the couplers increase or decrease through the device.

Two such filters—an up-chirp unit with flat amplitude weighting and ■ down-chirp with Hamming weighting—were produced. Both had bandwidths in excess of 2.5 GHz centered at 4 GHz, ■ shown by the upper two curves on the right in Fig. 5. The high degree of pulse compression, exhibited by the two filters in cascade, shows how well the filters met their design specifications [Fig. 5, bottom right].

CIRCUIT SOPHISTICATION. Unlike the other three projects, the circuits program focuses on pushing low-temperature superconducting devices to higher levels of sophistication. Such a program, it is hoped, will provide



[5] This YBCO chirp expander filter has 1.5 ns of dispersive delay. The top and middle curves compare the designed and measured responses of the expander and ■ compressor, respectively. The excellent matching allows the two filters to be operated as an expander-compressor pair [bottom].



ideas that could be applied to high-temperature superconductors in the future.

The most impressive first-year result of this program was the development of a three-layer process for building ultralow-noise Squids. Before the consortium was formed, IBM and Lincoln were fabricating devices using niobium-lead alloy and niobium-lead junctions, respectively. But neither institution had the resources to advance its process significantly or to explore the possible benefits of junctions in which both components (not just the niobium) were refractory materials.

By combining resources within the CSE, that problem has been overcome, and a world-leading all-refractory process based on niobium/aluminum oxide/niobium trilayers is being developed. As part of the effort, a multitarget sputtering system at Lincoln was adapted to fabricate high-quality trilayers.

In addition, a fast-turnaround IC fabrication process was developed for building structures on 50-mm wafers. The process uses four lithographic levels and can produce features as fine as 2 μm.

Using the trilayer process, various structures, including Squids, were built and then tested in collaboration between IBM and Lincoln researchers, who worked at both places. Some of the Squids that resulted exhibited lower 1/f noise than the old IBM Nb/Pb alloy process, which had been the world-leading process for Squids with low 1/f noise. It was the first demonstration of such low 1/f noise in a $Nb/Al_2O_3/Nb$ process, and encouraged the CSE to proceed in further developing low-temperature trilayer technology.

Consortium for Superconducting Electronics: progress so far

Program focus	First year	
	Goals	Accomplishments
Materials and processes		
Substrates	Modest-ϵ substrates for YBCO films, one of the substrates scaled to diameter of 50 mm	• 50-mm diameter $LaAlO_3$, $LaGaO_3$, and untwinned $NdGaO_3$ • New substrates[a]: $NdAlO_3$ and $LiBaF_3$
Films	High current density (J_c) for several systems	• YBCO: J_c (77K) > 1 MA/cm² • BSCCO[a]: J_c (77K) > 100 kA/cm² • TBCCO: J_c (77K) > 500 kA/cm² • New films: $Ba_{1-X}K_XBiO_3$
Processing and multilevel structures	Epilayer insulators	• $PrBa_2Cu_3O$ on YBCO • $SrTiO_3$ on YBCO
Junctions		
Junctions and weak links	Weak-link fabrication	• Natural junctions: —grain boundaries in YBCO, BSCCO, and TBCCO —BKBO/native-oxide barrier/BKBO (bulk) • "Engineered" edge junctions: —YBCO/BaF_2 (or $PrBa_2Cu_3O$)/YBCO
High-temperature (T_c) Squids	Flux transformer	• Natural-junction superconducting quantum interference devices (Squids) in YBCO and TBCCO • Engineered edge-junction Squid (to 60 K) • Hybrid YBCO coil and TBCCO Squid
Exploratory devices	Assessment of superconducting-channel FETs	• Conductivity modulation[a,b] • Proximity effects[a,b]
Networks		
Digital packaging interconnects	Coplanar transmission line	• Terahertz propagation in YBCO • Coplanar long-distance lines
Analog transmission lines	Stripline resonator	• High-Q resonator in YBCO[a,b] (Q = 1.5 x 10⁴ at 77 K, 1.5 GHz) • Delay line in YBCO[a,b] (7 ns long, operated with GaAs circuit)
Filter networks	Low-loss filter	• Four-pole filter[a,b] (0.3-dB loss at 77 K, 4.2 GHz) • Six-pole filter[a,b] (1.0-dB loss at 77 K, 4.7 GHz)
Circuits		
Low-T_c Squid arrays	Coil with submicrometer wire	• Three-layer Squids with ultralow 1/f noise built and tested[a,b] • 2-μm coils built and tested (0.1–0.7-μm coils built)[a,b] • Gradiometers built and tested[a,b] • Fully scalable process demonstrated (see below)[a,b]
Low-T_c transient sensors	Initial design	• Initial cell designs[a]
Advanced low-T_c facilities	Selectively scaled submicrometer technology	• Fast-turnaround three-layer process (2x2-μm junctions)[a,b] • Planarized three-layer process (0.7 x 0.7-μm junctions)[a,b] • Fully functioning circuits[a,b] (in both processes)

a These accomplishments can be attributed to the existence of the Consortium for Superconducting Electronics (CSE)—that is, they are not extensions of base activities.
b These accomplishments involved contributions by two or more CSE members.

TERRIFIC TRILAYERS. That development has proceeded apace. The Lincoln sputter film deposition system was modified to produce optimized trilayers on 125-mm wafers. IBM then developed a sophisticated planarized process for the trilayer wafers using state-of-the-art fabrication equipment in the advanced silicon pilot facility at IBM's Thomas J. Watson Research Center in Yorktown Heights, N.Y.

The combined approach has proven extremely successful. Squids, gradiometers, oscillators, and other devices, along with high-quality junctions down to 0.7 by 0.7μm, were demonstrated in short order [Fig. 6]. Significantly, the low-noise characteristics of the trilayers were maintained through the processing required to produce planarized submicrometer circuits.

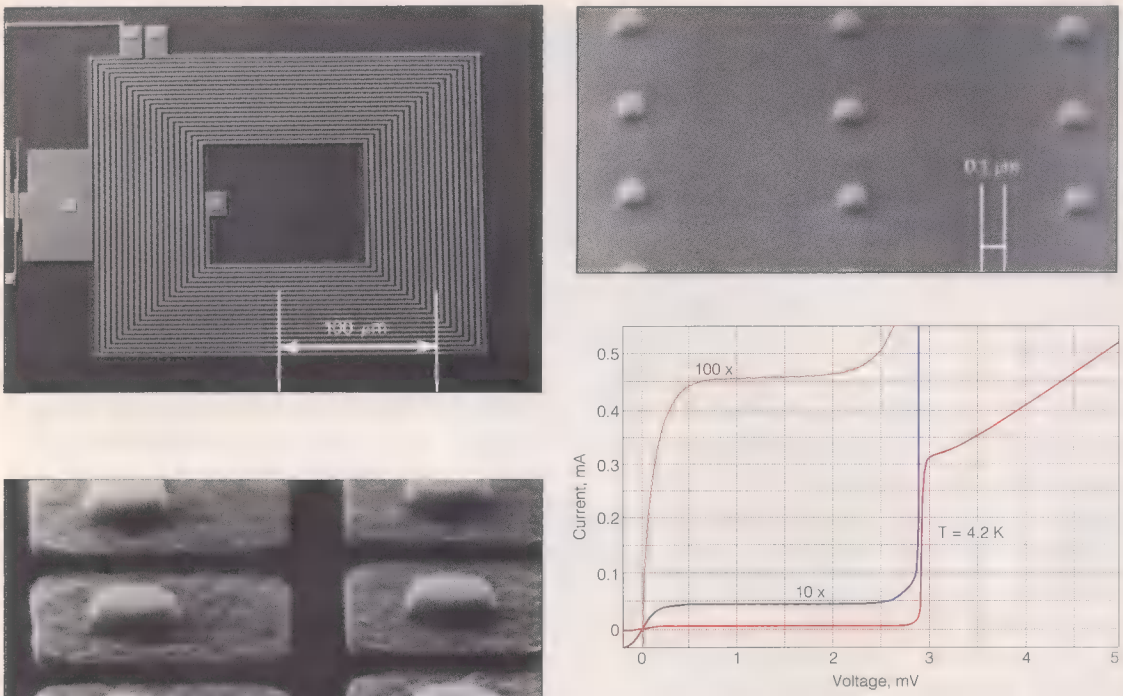
Of course, to scale the junction part of this technology to the deep submicrometer regime, it will be necessary to obtain higher current densities in the trilayers. That will necessitate making aluminum oxide tunnel barriers even thinner than the few nanometers that have been achieved so far—down to a few tenths of a nanometer—a task that cannot be done in reproducible fashion with the Lincoln system.

The machine required to grow the improved trilayers has been purchased by AT&T and installed there, where it will serve the needs of both the CSE and the local research community.

SPEEDY COLLABORATIONS. Much of the research within the CSE has become collaborative in a remarkably short time. The Darpa funding has been used, wherever possible, to partially support Lincoln Lab and MIT researchers involved in collaborative projects as well as research assistants jointly supervised by MIT faculty and scientists at AT&T, IBM, or Lincoln.

Three new university members of the CSE—Cornell University, Boston University, and the State University of New York at Stonybrook—are also bringing important contributions to all four programs. Overall, about two-thirds of the CSE projects involve more than one institution, and the four original members are each involved in all four programs.

One example of the benefits of this collaborative mode of research and education involves a graduate student at MIT who has begun exploring the possibility of making a superconducting field-effect transistor (Sufet). The student works with IBM scien-



[6] Photos of $Nb/Al_2O_3/Nb$ trilayer structures show the coil and junction regions of a Squid [top left], an array of 0.7-μm junction pedestals [left], and 0.15-μm dots [top right]. Note the excellent I-V characteristics of a 5-μm junction.

tists to fabricate devices, and then with scientists at AT&T Bell Labs, where the devices are tested. The benefits are at least twofold: the work is proceeding more rapidly than it otherwise would, and the student is being exposed to a wider variety of outstanding researchers than is usual in graduate work.

FUNDING SOURCES. The Darpa funding of the CSE began in February of 1990 and totaled US $3.9 million for the first year. A conservative estimate of the industrial contribution is that IBM and AT&T are each contributing $2 million annually, not counting capital equipment. In addition, the industrial members contribute $300 000 the first year and $100 000 per year thereafter, in part to support student and post-doctoral researchers at the industrial laboratories.

It is not expected that the CSE will have more than a few new members, and probably none as large as the original four. In addition to the three universities that began participating during the first year, Conductus Inc., Sunnyvale, Calif., a small industrial firm, joined the CSE in October 1991. Conductus is now participating in microwave circuit development in hopes of quickly coming up with a commercial product. It is also playing a role in the shared research.

The transition to practical products is of great concern to the CSE partnership. Coincidentally, early successes in commercialization should help ensure continued funding of the pre-competitive activities that must precede a buildup of any commercial operations.

ACKNOWLEDGMENT. The authors thank all their colleagues who have contributed to the results summarized here. They also acknowledge the help of M.B. Ketchen, J.M. Phillips, and R.S. Withers in preparing this report.

TO PROBE FURTHER. A good basic text on superconducting devices is Theodore Van Duzer and C.W. Turner, *Principles of Superconductive Devices and Circuits* (Elsevier North Holland Co., New York, 1981). Engineer readers may find the language more accessible in the following book, since it was written for use in the Massachusetts Institute of Technology's department of electrical engineering: Terry P. Orlando and Kevin A. Delin, *Foundations of Applied Superconductivity* (Addison-Wesley, Reading, Mass., 1991).

Another good source is S.T. Ruggiero and D.A. Rudman (eds.), *Superconducting Devices* (Academic Press, New York, 1990).

The *Proceedings of the IEEE*, special issue on superconductivity, Theodore Van Duzer and Clyde E. Taylor (eds.), Vol. 77, August 1989, covers both low- and high-temperature superconductivity. The applications covered in the special issue primarily involve low-T_c superconductors because most of the high-T_c work at that time focused on materials development. For more information on applications of high-T_c superconductivity, especially filters and antennas, see the *IEEE Transactions on Microwave Theory and Techniques*, special issue on microwave applications of superconductivity, Vol. 39, September 1991.

ABOUT THE AUTHORS. Richard Ralston has been the leader of the Analog Device Technology Group at MIT Lincoln Laboratory, Lexington, Mass., since 1984. His duties include managing the development of semiconductor and superconductive electronics, with emphasis on signal-processing applications. Since 1989, he has also served as the principal director of the Consortium for Superconducting Electronics, which is headquartered at Lincoln.

Marc A. Kastner is Donner Professor of Physics at the Massachusetts Institute of Technology, Cambridge. His research interests include the study of the physics of the layered copper oxides and the electronic properties of nanometer-sized semiconductor devices. His research within the consortium has focused on an effort to fabricate a superconducting field-effect transistor. He was an associate director of the Consortium for Superconducting Electronics through January 1992.

William J. Gallagher is a research staff member and manager of the Exploratory Cryogenics Group at IBM Corp.'s Thomas J. Watson Research Center in Yorktown Heights, N.Y. He is also an associate director of the Consortium for Superconducting Electronics. His areas of specialization are superconducting electronics, especially Squids, and the electromagnetic properties of superconductors.

Bertram Batlogg heads the solid state and physics of materials research department of AT&T Bell Laboratories, Murray Hill, N.J. His research efforts have centered mainly on materials-related solid-state physics with emphasis on systems dominated by strong correlations among the electrons. Most recently, they have also included the physics of high-temperature superconductors and their applications potential. ◆

Measuring software reliability

Code must be reliable from the surprisingly divergent viewpoints of software developers, testers, and users

Software reliability can mean different things to different people in different situations. A software developer, who views code as instructions to hardware, may judge them reliable if each software requirement is executed properly by a related set of those instructions. A user sees the same software as a set of functions and deems it reliable if nothing malfunctions.

The two viewpoints may yield contradictory estimates of the same software's reliability. For example, someone placing a telephone call at a time when all circuits are busy may be dropped mid-call by a system seeking to balance the load on the overall system and keep as many people as possible on the line. To the caller, the system looks unreliable; to the developer, it is working exactly as required.

Conversely, the same person calling from New York City to San Francisco is happy to find that calls always go through. But because of a fault in the system, all calls between those two points are routed through Chicago. The user thinks the system is reliable, but the phone company staff who maintain the system see the unusually high volume of traffic through Chicago and know something is wrong.

Examining the component concepts of that vague term "reliability" should clarify why its measurement is difficult. It should also reveal what issues require further exploration and definition before reliability measurement becomes as straightforward for software as for hardware.

MANY PRODUCTS. The notion of software reliability borrows heavily from its counterpart in hardware: a reliable system is one that works correctly over a long period of time. But in hardware, the final product—say, an automobile—is not the only product of development. There are many intermediate products: the requirements that specify the automobile's characteristics and functions, the architectural layout of its parts and wiring, and the prototype built to test the reliability of the design before it enters manufacture. The final car will not be reliable unless the requirements, the design, and the individual parts are all reliable.

Similarly, computer code—1s and 0s—is only the final product of software development. The intermediate products are the requirements specifying the functions the software must perform; the design drawn from the requirements and used by the programmers to generate code; and even the plans for testing the software.

All those intermediate products of development can and should be considered when evaluating a software system's reliability. The requirements specify how reliable the code must be. The design must implement the requirements in such a way that the specified reliability is likely to be achieved. The test plans measure how well the code meets the requirements.

FINDING THE SOURCE. But testing may uncover not just mistakes in the code but also problems with the design and the requirements. Since correcting a problem in the requirements costs only 1 percent as much as fixing code, early reliability prediction can save money and time.

> Fixing a problem in the requirements costs 1% as much as fixing the resulting code

To describe problems in software, the IEEE/American National Standards Institute (ANSI) Standard 982.2 distinguishes among errors, faults, defects, and failures. While all the definitions are related, differentiating among them assists software developers in pinpointing the source of a problem.

According to the IEEE/ANSI standard, an *error* is a human mistake that results in incorrect software. For example, a user may have omitted a critical requirement in the software specification, so that the software developers design an inappropriate product. Similarly, the developers may have misinterpreted a requirement, or translated incorrectly from design to code.

The resulting *fault* is an accidental condition that causes a unit of the system to fail to function as required. Thus, the fault is a manifestation of an error in the software. Sometimes, faults are called bugs—parts of the software needing to be fixed.

Faults often lead to a *defect*—an anomaly in a product. Defects include problems not only with the code (the final product) but also with the design and requirements (intermediate products). Defects include an ambiguous requirement, an omission in a design document, a fault in code mature enough for test or operation, an incorrectly specified set of test data, an incorrect entry in the user documentation, and more. And it is defects that lead to failures.

A *failure* occurs when a functional unit of the software-related system (including the software-driven hardware) either can no longer perform its required function, or cannot perform it within specified limits.

CAUSE AND EFFECT. Human errors, software faults, and product defects describe the causes of problems, whereas functional failures describe the effects.

The cause of each problem must be traced to its root, because that determines the problem's impact on system reliability. A design flaw is often more serious than a simple software fault. Consider an analogous situation in automobile production, where testing has shown that a new car is likely to explode when hit from behind. If the root cause is that the gasoline tank is made from inferior metal, then the solution may simply be to find a new metal supplier. However, if the root cause is faulty design—the placement of the gasoline tank—then the automobile may need total redesign.

In the same way, an intermediate product may be ultimately responsible for unreliable software. A human may misinterpret a critical requirement, leading to a bad design, resulting in bad code. Such a chain of events is often harder to remedy than a misplaced comma in code.

Note that faults, defects, and failures represent dissimilar points of view. Faults and defects are what the developer and maintainer see: they view the system from the inside out, tracking faults and defects to find the cause of problems. On the other hand, failures represent a user's view of the system: the concern is how the system functions (or fails to), regardless of cause.

An error can occur from either point of view. The user may err in specifying the requirements for a system or in using the system. Alternatively, the developer may code

Shari Lawrence Pfleeger Mitre Corp.

0018-9235/92/$3.00©1992 IEEE

incorrectly or misinterpret a requirement. Either error can lead to faults and/or failures.

TOUGH TO MEASURE. The distinctions among errors, faults, defects, and failures are important because reliability, often viewed in terms of software faults (the developer's view), is officially defined in terms of functional failures (the user's view).

As defined by IEEE/ANSI Standard 982.2, software reliability is "the probability that software will not cause the failure of a system for a specified time under specified conditions." This definition parallels that of the hardware world. But any attempt to measure software reliability quantitatively, according to the standard IEEE/ANSI definition, runs into several problems.

First, the standard IEEE/ANSI definition is not accepted by everyone who writes reliability requirements. The interpretations of the term as expressed in user requirements are many and varied. Some indeed follow the IEEE/ANSI definition and deal with the user's view of the system (looking at failure information). Others focus on characteristics of the code as seen by the developer (looking at faults). Different measures may be needed to capture each.

Second, the standard requires tracking the use of the system over time while noting the number of failures. But when reliability requirements are strict, it may be impossible to test the system for long enough to verify a very low probability of failure. Or the system may be untestable in the field, as are several of the systems proposed for the U.S. Strategic Defense Initiative.

Perhaps most serious, the standard IEEE/ANSI definition requires the system to be completely designed, developed, and operational before reliability can be measured. That leaves developers with no direct, preliminary measures of reliability while the software is being written—even though software is harder and more costly to fix when complete than while still in development.

REAL WORLD. Broadly speaking, there are two approaches to measuring the reliability of finished code. The first, a developer-based view, focuses on software faults; if the developer has grounds for believing that the system is relatively fault-free, then the system is assumed to be reliable. The second, a user-based view more in keeping with the standard IEEE/ANSI definition, emphasizes the functions of the system and how often they fail.

In the first approach, the developer may collect information about fault density: the number of those faults discovered per 1000 lines of code. The developer then tracks the total number of unique faults in a given time interval. This number of faults divided by the total number of lines of code in the final product yields the fault density. By comparing fault density numbers for similar systems, the developer can judge whether the current system has been tested thoroughly. In addition, the developer can infer the likely reliability of the software once it is installed in the field.

Alternatively, the developer may use a technique called fault seeding to estimate the number of faults remaining in the existing software. The quality-control team deliberately inserts into the software faults representative of the kinds observed to have occurred in the past (such as transposed 1s and 0s, or an incorrect exponent, or a branch to a wrong place in the code). The distribution of the faults matches the probability distribution previously observed on similar projects.

Then, the test team searches the code for all faults. In theory, if they discover all the seeded faults, the testing has been thorough enough to uncover all the accidental unseeded faults as well. The ratio of discovered non-seeded to seeded faults is taken to indicate the number of faults remaining in the code, the thoroughness of testing, and—indirectly—the system's reliability.

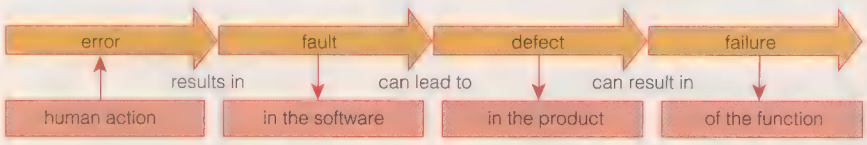
THE FAULT WITH FAULTS. The problem with the fault-seeding approach is that it does not look at failures in any context. Faults may exist in the code but not affect user function (for example, in income-tax-computation software, a fault may cause certain programmed equations not to work in the case of someone having negative income—but since no one has negative income, the fault does not matter). The system is thus faulty but reliable, according to the standard IEEE/ANSI definition.

1. Some existing software reliability indicators

Measure	Purpose	Definition	When to use
Required reliability	Indicates requirements for reliability	Quantitative rating from very low to very high, based on Cocomo cost driver[a]	For the requirements specification
Run reliability	Predicts final software reliability	Given k randomly selected runs during a specified time, probability that all k runs give correct results	Whenever set of possible discrete input patterns and states is well-defined
Fault density	Predicts remaining faults	Number of faults divided by thousands of lines of code (reported by severity level[b])	During testing
Mean time to discover next k faults	Predicts time to reach reliability goal	Based on certain reliability models, observed times until last failure divided by number of failures from start of test to now, plus observed time between the two failures	During testing
Independent process reliability	Measures service reliability	Sum of correctness delta function weighted by user profile[c]	During testing, when processes are still logically independent and can be tested separately
Failure rate	Indicates growth in reliability as a function of test time	Cumulative probability distributions based on certain reliability models	In acceptance testing
Mean time to failure	Predicts stability of system	Mean observed times to next failure (either clock time or execution time)	In acceptance testing

a Cocomo stands for Constructive Cost Model, a cost-estimation technique.
b Severity level is how much impact a failure may have on a system ranging from, for example, loss of income through loss of subsystem function or of total system to loss of life.
c The correctness delta function maps a correct response as 1, an incorrect one as 0, weights the results by the likely use of each function, and adds them to yield a figure of merit.

Defining terms



Error: any human mistake that results in incorrect software; errors include an omission of a critical requirement in a software specification, a developer's misinterpretation of the requirement, or an incorrect translation from design to code.
Fault: an error's manifestation in software that causes a functional unit of the software system to fail in performing its required function; sometimes called a "bug," a fault is a part of the code that needs to be fixed.
Defect: an anomaly in any intermediate or final software product resulting from an error or fault, ranging from an incorrectly specified set of test data to an incorrect entry in user documentation.
Failure: inability of a functional unit of the system depending on the software to perform its required function, or to perform the function within required limits.

Moreover, all the fault-based techniques can be misleading: the fact that many faults are discovered can mean that testing is thorough; but it can also mean that many more faults remain in the code.

For this reason, John Musa, supervisor of software quality at AT&T Bell Laboratories in Whippany, N.J., and others have concentrated on a failure-based approach to reliability. Musa broke new ground in 1975 by defining software reliability as how closely user requirements are met by a computer program in actual operation. His definition incorporates the profile of the user's probable usage of the various system functions (an "operational profile") and counts in only the time the system is running, rather than clock time. Musa suggested that reliability be considered as the probability of failure-free operation of a computer program for a specified time—for example, software reliability of 0.92 for 8 hours of execution.

One technique uses failure profiles, tracking failures in several categories of severity level. That is, failures can be classified in terms of the severity of their effect(s) on the system. For example, developers of a telecommunications system may use three levels of severity. Level 1 is minor, resulting at most in loss of income (example: system consistently underreports connection time by one minute when billing). Level 2 is major, producing partial loss of function (example: system cannot forward calls for all exchanges). Level 3 is critical, entailing total loss of a key function (example: no calls can be made to the East Coast). Cumulative failures may be tracked over time, where time may be measured in a variety of ways, including execution time, clock time, and usage time. The failure profile may be viewed for the overall system, for subsystems, and even for modules. The shape of the resulting curve is then used to project when testing will be complete, assuming sufficient test coverage.

Another technique is the analysis of time between failures. A model of failure rate is chosen (based on which models have been most accurate for similar software applications), and estimates are made of initial fault content (number of faults), normalizing constants (distribution of faults throughout the code), and initial mean time to failure. The model is then used to estimate the number of remaining faults, the ultimate mean time to failure, and hence the system's overall reliability.

Many such failure-rate models exist, including some based on mathematical models of a non-homogenous Poisson process and on a Bayesian model. As might be expected, choosing the correct model is a challenge with failure-based approaches.

All those approaches, however, depend on the software system's being nearly complete and look primarily for mistakes in the code. Ideally, well before the system is cast into code, there should be some way of evaluating the reliability of all the early and intermediate products, including the requirements and the design, so as to predict the reliability of the code.

As of now, no proven ways exist of evaluating the reliability of a system's requirements or design. At best, the probability that the design will result in reliable code can be assessed only in terms of measurements that may indicate the likely reliability. Examples are design complexity, the number of defects discovered in a design review, or the density of defects relative to some measure of the design's size [Table 1].

Note that none of these indicators is a direct measurement of reliability, nor is any of them a foolproof, accurate predictor of the required reliability. Neither do developers always have methods to examine intermediate code products to reassure them that the final code will meet the system's reliability requirements. At best, intermediate indicators suggest trends.

Thus, although reliability can be expressed in quantitative terms when defining the system's requirements, there are only indirect ways of controlling this feature during the system's development. Furthermore, although it may be possible to measure the completed system's reliability, it may not be possible to change the system at that point if it is found to be unacceptable.

> Ideally, there should be some way of evaluating the reliability of the requirements and design

THEORY VS. PRACTICE. This gap between theory and practice—between predictions of reliability from indirect indicators (such as the number of design defects) and actual measurements of reliability (such as the number of failures over time)—is quite wide and narrowing very slowly. Several circumstances contribute to this situation.

First, regardless of whether reliability is defined in terms of software faults or functional failures, it is difficult to generalize from measurements of the reliability of software subsystems to the likely reliability of the system as a whole. There are a host of reasons, among them the fact that the reliability of the individual units indicates nothing about the reliability of the connections and sequencing among units.

2. Levels of reliability of code

Type of testing	What is tracked	Reliability measured			
		Modules	Subsystems	System	Functions
Unit	Faults	X			
Integration	Faults	X	X		
System	Faults	X	X	X	
Acceptance	Failures	X	X	X	X

More fundamentally, Maria Teresa Mainini of Esacontrol, Genoa, Italy, and Luc Billot of CISI Ingénièrie, Rungis, France, point out that testing various subsets of the system actually conveys different views of reliability and different test results [Table 2]. Unit testing, integration testing, and system testing, for example, which each focus on identifying software faults, say something about the reliability of individual modules, of subsystems (that is, collections of reliable modules) and of the system, respectively. But it is not until acceptance testing that the test team looks directly at functional failures to evaluate the system's actual operational reliability and to verify its functionality is as specified in the requirements.

To be sure, in some cases the earlier measures (of faults) can be linked to predict what later measures (of failures) are likely to be. But as pointed out earlier, faults in the code are not the only causes of failure. For example, users may misuse the system because of a poor design. Thus, the indicators of software reliability should be viewed in the context of what question is being asked. Otherwise an inference about ultimate reliability from earlier indicators could be inappropriate.

Finally, even when there is agreement on a definition of reliability and it is measured in the correct context, a simple measure may not be enough to capture the measurer's intent. If so, it is better to view reliability as a composite of measures of the various products of development in the context of the reliability goals. In fact, in many cases, the reliability of the earlier products sets an upper limit to the reliability of the final product. For example, an inherently unreliable design may never yield reliable code.

A composite approach to reliability is timely. For years, software engineering researchers have defined simple one-dimensional metrics to measure complex things: usability, design complexity, maintainability, and more. Only now are researchers acknowledging that a broader perspective is needed. The simple measures must be combined to form a multidimensional composite, and for complete understanding, each measure must be interpreted in context.

THREE LEVELS OF MEASUREMENT. At least three steps are needed to implement this composite approach for reliability indicators at the early stages in software development, as well as help developers choose which set of mathematical models is appropriate in the

evaluation of software faults or functional failures at later stages. The steps involve defining reliability, identifying what about it needs to be known, and then measuring a variety of characteristics that help answer critical questions [Table 3].

Step one is crucial, since reliability presents a different aspect to developer, maintainer, and user. Each definition must be placed in the context of an overall system view of someone who understands the need for reliability.

The importance of this top level cannot be underestimated. Consider what happens when an error occurs in an airplane's software. Usually, the supporting system tries to compensate so as to maintain system integrity. No general, systemwide failure occurs; the plane must keep flying no matter what, so each contributing subsystem must keep working.

In a telephone system, though, a similar error is usually handled by restarting an entire system or subsystem: the problem call is dropped, and the remaining system is intact. Such an approach is appropriate for communications but is out of the question for aerospace applications. Each system's needs dictate opposite interpretations of reliability.

Next, at the middle level of the reliability measurement framework, the overall definition of reliability is used to develop a model of the system from a given viewpoint. The model should show how and when the viewer must predict or verify the current reliability of the system. To illustrate, a system model can show how reliability is assessed from the design, is predicted from design and code characteristics, and improves during testing. This model makes it possible to determine the reliability goals of the system and to pose questions about those goals that measurement can answer.

To revert to the phone system and airplane: the model for the first reflects the definition that a failure may be counted only when the entire system ceases to work,

3. Three levels of reliability measurement

Defining what is meant by reliability

Beholder	View	Model	Definition
User	Pilot	Airplane is a collection of interdependent key subsystems	Total system works properly
	Telephone caller	Network is a collection of independent but connected subsystems	A chain of subsystems works properly
Developer	Airplane control software developer	Software controls a collection of interdependent key subsystems	All key subsystems work properly
	Switch software developer	Software connects available independent subsystems	At least one chain of key subsystems works properly
Maintainer	Airplane control software maintainer	Software enhancement at the least maintains system reliability by maintaining or increasing the reliability of each key subsystem	Same as for airplane control software developer
	Switch software maintainer	Software enhancement at the least maintains system reliability by maintaining or increasing the number and reliability of connections	Same as for switch software developer

Setting reliability goals

Beholder	Reliability view	Reliability goal	Reliability questions	Reliability indicators/measures
Pilot	Sees airplane as the sum of its subsystems	Maintain flight	Can plane maintain flight at all times?	Number of failures of total system over time Number of failures of key subsystems over time
Telephone caller	Sees telephone system as a connection between self and called party	Obtain and maintain connection	Can caller be connected with called party? Can caller and called party stay connected for duration of call?	Number of disconnects (failures) over time
Airplane control software developer/ maintainer	Sees airplane as a sequence of interdependent subsystems (sequential reliability)	Maintain flight	Can overall system maintain flight? Can key subsystems meet required reliability?	Number of failures of total system of time Number of failures of key subsystems over time Number of faults discovered per subsystem Depending on goals, reliability of system can be the minimum, maximum, or product of subsystem reliabilities
Switch software developer/ maintainer	Sees telephone system as a multitude of parallel connections (parallel reliabilities)	Maintain maximum number of connections	Does any new connection lower system reliability? What is the minimum acceptable system reliability?	Number of failures (fewer than acceptable connections) over time Number of individual connections dropped over time Depending on goals, reliability of system can be the minimum, maximum, or product of 1 minus subsystem reliabilities

Measuring reliability (at any stage)

Set initial goals for software reliability
→ Collect data on early software products (e.g., design defects)
→ Analyze data for indicators of reliability of final system
→ Predict reliability of actual system
→ Develop final code
→ Collect faults/failures data
→ Analyze data for actual reliability
→ Revise reliability goals, if necessary
→ Answer reliability questions
→ Correct code
→ Meet reliability goals

How much testing is enough?

When is software deemed to be reliable enough to release to the customer? Software developers vary in how they combine software-reliability measures and models to make that decision. One decision technique is the zero-failure method of Motorola Inc., headquartered in Schaumburg, Ill., outlined by Ralph Brettschneider in the July 1989 issue of *IEEE Software*.

The zero-failure method specifies the number of hours of testing needed without a failure before the software is deemed ready for release to the customer. If even one failure is detected during this target test time, then the request for release to the customer is denied and testing must be continued.

According to Brettschneider, the zero-failure method—like other reliability models—is based on several key assumptions, of which two are particularly important.

First, the longer that testing proceeds without a failure, the more likely it is that the number of failures remaining is very small. Specifically, the zero-failure method assumes that the rate at which failures are discovered decreases exponentially as testing progresses.

Second, the zero-failure method assumes that testing is representative of the actual use of the software in the field, and that the probability of discovering failures is constant and equal for all kinds of failures.

To apply the method, Motorola sets a reliability goal in terms of an average number of failures per thousand lines of code. To calculate the number of failure-free test hours required, three inputs are needed: the permissible average number of failures due to faults embedded in the code sent to the customer; the total number of test failures detected so far; and the total number of hours the software has been tested up to the discovery of the last failure.

The Motorola zero-failure method sets forth a formula for calculating the number of hours needed to test without failure before the software can be deemed reliable.

As an example, Brettschneider considered a 33 000-line revision to a program. Up to now, 500 hours of execution time have revealed 15 repairable failures. No failures have been discovered in the past 50 hours since the last repair. If the goal is to deliver a product with no more than one failure (1 out of 33 000 lines or 0.03 failure per thousand lines of code), has the software now been tested enough?

Using the formula, Brettschneider showed that Motorola's test organization must test the 33 000 lines of code for another 27 hours with no failure discovered before the software is deemed ready to ship to the customer. If a failure occurs, however, the clock must be reset and testing must continue until there are 77 continuous hours without a failure.

Brettschneider's example shows that while measurement cannot ensure reliability, it can guide the development process and minimize the probability of unreliable software. Just as Motorola has done, other software developers can build or borrow a reliability model based on past experience and use it to increase confidence in the effectiveness of their testing. —*S.L.P.*

whereas the model for the airplane deems it a failure when any key function stops working correctly.

Finally, the bottom level addresses the actual measurement values. During data collection and analysis, where information is gathered to instantiate the model, questions are answered, the answers viewed in the context of the overall system, and decisions made accordingly. At this lowest level, the measures of reliability may support quite contrary decisions for seemingly comparable failures. In the extreme, a telephone system with 100 dropped calls (partial failures) and zero complete system failures may be considered reliable, while an airplane with the same track record may be a dead loss.

Approaching reliability in this way provides a three-level framework for the process of reliability measurement: build a process or system model to depict the relevant issues, decide what questions are to be answered and define measures that address the questions, and gather information to help find the answers.

BURNING ISSUES. Models and measures of hardware reliability have been invaluable in assuring users that their hardware will function properly over time. So it is encouraging that the same notions are being applied to software reliability in the hope of generating similar assurances—especially when software has become a key part of almost all systems that are in use today.

But current efforts have a long way to go. Close to home, the telephone system is still subject to embarrassing failures due to unreliable software: a widespread telephone outage in June and July 1991 was caused by one line of a subcontractor's code that had not been tested thoroughly ["Faults & failures," *Spectrum*, May 1992, p. 52].

Clearly, several issues must be addressed, or addressed more completely, before complete confidence can be reposed in the ability to predict and measure software reliability. At a minimum, researchers must:

- Build a family of traditional and nontraditional models of reliability, including parameters to determine which model is best for a given situation.
- Generate indicators of reliability early in the development process.
- Define the reliability of artifacts other than code.
- Determine composite measures of reliability that reflect the reliabilities of related artifacts.
- Suggest additional techniques for using reliability information to guide software development and maintenance.

This blueprint for the future suggests areas for researchers to investigate.

TO PROBE FURTHER. The 1988 *IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software, IEEE Standard 982.2*, discusses almost three dozen commonly used indicators of reliability, summarizing the underlying theory and giving examples of how the indicators can be used.

Bev Littlewood, in his article "Theories of Software Reliability: How Good Are They and How Can They Be Improved?," discusses the pros and cons of several popular models of software reliability. The paper was published in *IEEE Transactions on Software Engineering*, Vol. SE-6, no. 5, September 1980, pp. 489–500.

Ralph Brettschneider, in "Is Your Software Ready for Release?," published in the July 1989 issue of *IEEE Software*, pp. 100, 102, and 108, gives a concrete, mathematical example of how a tailored reliability model is used to decide when testing is complete at Motorola Inc.

In the January 1990 issue of *Software Engineering Journal*, Vol. 5, no. 1, pp. 27–32, Maria Teresa Mainini and Luc Billot in their paper "PERFIDE: An Environment for Evaluation and Monitoring of Software Reliability Metrics During the Test Phase" supply an example of the actual tools and techniques used to evaluate reliability on a large project.

John D. Musa's seminal paper on defining reliability as a measure of how closely user requirements are met is "A Theory of Software Reliability and its Application," published in the *IEEE Transactions on Software Engineering*, September 1975, Vol. SE-1, no. 3, pp. 312–27.

Musa, Anthony Iannino, and Kazuhira Okumoto, in their textbook *Software Reliability: Measurement, Prediction, Application* (McGraw-Hill, New York, 1987), survey numerous leading approaches to the subject, including the development of an operational profile, choice of a reliability model, and use of the profile and model to guide software testing.

Musa summarized some of his approaches in "Tools for measuring software reliability," published in *IEEE Spectrum*, February 1989, pp. 39–42.

The second edition of *Software Engineering: The Production of Quality Software* (Macmillan, New York, 1991) by the author of this article discusses reliability in the context of the overall software development process.

ABOUT THE AUTHOR. Shari Lawrence Pfleeger (M) is a principal scientist at Mitre Corp.'s Software Engineering Center in McLean, Va., whose current research focuses on software metrics and the software development process. The author of two textbooks and more than two dozen journal articles in mathematics and computer science, Pfleeger's numerous IEEE activities include being a member of IEEE Software's Industrial Advisory Board. She also is a member of the Association for Computing Machinery, where she chairs the Committee on the Status of Women and Minorities in Computing. ◆

FOCUS REPORT

SPECTRUM'S 1992 ENGINEERING/SCIENTIFIC SOFTWARE REPORT & GUIDE

SOFTWARE

DESIGN, MATH, GRAPHICS AND MORE

WHAT'S UP IN ENGINEERING/SCIENTIFIC SOFTWARE?

ANNOUNCING SPECTRUM'S THIRD ANNUAL FOCUS REPORT & GUIDE TO ENGINEERING/SCIENTIFIC SOFTWARE-NOVEMBER 1992

An update on what's new and what's vital for today's computer-aided design and engineering professional. Up-to-the minute tabulations that integrate key data and information on the most advanced engineering/scientific software packages for PCs and workstations.

Eminent authors and reviewers assess the advantages—and some disadvantages—among the following product categories:

- Logic synthesis for ASICs
- Mixed signal and analog design
- Electromagnetic simulation and design
- Multichip module routing and placement
- Data handling (acquisition, analysis, display and technical reporting)
- Math, graphics, visualization
- Development tools for embedded signal processing
- CAD frameworks

Plus two new, special features:

- Report on SPECTRUM's subscriber survey on software usage
- Report on users panel on framework utilization

Don't miss this exclusive, high profile marketing environment in our November issue. It's your opportunity to reach the core of the high-tech software market, over 320,000 SPECTRUM subscribers—100% engineering/scientific audience —the largest single concentration of electronics, communications, computer and high technology professionals in the world.

For more information, contact a SPECTRUM Regional Sales Office.

Issue date November 1992 **RESERVE SPACE NOW!** **Ad closing date: October 1**

IEEE SPECTRUM MAGAZINE

The High-Tech Marketing Tool™

345 East 47th Street, New York, NY 10017, U.S.A. 212-705-7760

Spectrum is published by The Institute of Electrical and Electronics Engineers. Inc.

Susan Hackwood

This former Bell Labs engineer is the founding dean of the first new U.S. engineering college in more than a decade

After decades of immersing herself in science fiction novels and rarely missing an episode of "Star Trek," Susan Hackwood is no longer much of a sci-fi buff.

"I discovered science fiction is a misnomer," she said. "It's really engineering fiction—engineers create those wonderful machines, those fascinating worlds."

These days Hackwood is creating her own fascinating world. She is dean of the first new college of engineering to be started in California in more than 30 years and in the United States in nearly 15 years. "I'd rather live engineering fiction than read it," she commented in her soft British accent, as she sat at her neat desk overlooking the verdant Riverside, Calif., campus.

It is here students in the new college learn about the environmental applications of all fields of engineering. They also work in a "systems clinic," an outreach program to local industry where they and faculty staff members help to solve real-world problems brought in by area companies. And their engineering curriculum includes studying Japanese so they can study abroad if they want to.

NO GIRLS ALLOWED. Growing up in England, Hackwood had a rough path to the world of her dreams. For the longest time, it seemed to her to be closed to women.

Her earliest career goal was to be an extraterrestrial veterinarian, a field she invented to combine her loves of futuristic science and animals. But Hackwood had a nose for the scent of solder—her father was a television repairman, and she herself was an incorrigible tinkerer. "I loved taking things to pieces, though I could never put them back together again," she recalled. One of her inventions as a child was a solar-cell–powered irrigation system that sensed dry soil and responded by triggering an old toilet flush.

Tekla S. Perry Senior Editor

Liverpool in the late '60s, however, did not encourage little girls to study science or technical fields, so the young Hackwood channeled her creativity into the more "appropriate" medium of kinetic sculpture. She planned to study art at a university, and at age 16 took and passed the fine arts entrance examinations. But since most UK colleges did not allow students to start until age 18, she registered for a few high school classes in science and mathematics.

There she quickly fell in love with science—the study of which, she felt, required more analytical brainwork than art did, and offered more opportunities to be inventive. (Though in her "Trekkie" days she identified more closely with the emotional Captain Kirk, she had always aspired to be more like the logical Mr. Spock.) She soon informed her high school career counselor she wanted a career in science. Then, the counselor responded, you ought to be a dental hygienist.

Hackwood was upset by this advice. The space race was under way, and science was opening up all sorts of new horizons. Though she did not follow the counselor's advice, it shook her confidence and prevented her from applying to Oxford and Cambridge universities. Instead she settled for a lower-tier school, Leicester Polytechnic Institute, where she studied chemistry and physics.

Halfway through her Ph.D. studies there, she moved from science to electrical engineering—a program she was able to enter only by promising to complete it before having any children. (Women are a risky investment, the Leicester Polytechnic faculty told her.) For her doctorate, she focused on solid-state ionics.

> "I never thought I'd get paid for doing this stuff"

At that point, she realized the difference between engineering and science. As she explained, "a scientist's mind is trained to unlock the secrets of the universe, and an engineer's mind is trained to synthesize new things from those secrets." Once that sank in, she knew that what she really wanted was to be an engineer.

Given a brief chance to study in the United States toward the end of her Ph.D. program, she was amazed, she recalled, not to "feel like a creature from another planet—there were other women doing what I was doing!" Not many, but a few.

TO MECCA. She "sprinkled America with résumés" and a few months later got a call from Bell Laboratories, Murray Hill, N.J., the mecca for an aspiring builder of future worlds. The company hired her as a postdoctoral researcher to work on ion insertion materials (specifically hydroxsyl and hydrogen ions for iridium oxide) for use in liquid-crystal–like display devices.

Hackwood began in January of 1980. "When they told me what my salary was, I thought they'd made a mistake with the zeros," she said. "I never thought I'd get paid for doing this stuff."

The level of intelligence of the workforce at Bell Laboratories proved exhilarating for Hackwood. "I don't think I slept for six months," she said. It was a highly productive time: she published prolifically and was awarded several patents. She found good mentors who, despite being "middle-aged white men," seemed blind to the fact that she was a woman.

One of those mentors, Robert Lucky, executive director of research, was so impressed he made her department head at age 28—the youngest person to hold that position at the time.

Hackwood blossomed at Bell Labs, she believes, because she felt that for the first time in her life, her only limits were her abilities, not her environment or the tools she could obtain to do her job.

I, ROBOT. After two years at Bell Laboratories, though her research in ion insertion materials was successful and she clearly had a bright future with it, Hackwood decided to make a drastic change in fields—to robotics. Perhaps it was because one of the few female engineers Hackwood had read about as a child was Isaac Asimov's fictional Susan Calvin, the robopsychologist in *I, Robot*. Or perhaps it was because she felt that the breakthroughs left to be made in ion insertion materials just were not earth-shattering, and she wanted a less limited playing field.

Whatever the reason, Hackwood chose robotics as her new technical specialty, one she felt was an important direction in which to head, even though it was considered a blue-collar type of engineering, with "tattoo-on-the-arm" scientists, she recalled.

"Susan sees opportunities long before other people do," Arno Penzias, vice presi-

Photo: Ron Mesaros

0018-9235/92/$3.00©1992 IEEE

Vital statistics

Name: Susan Hackwood
Date of birth: May 23, 1955
Place of birth: Liverpool, England
Height: 168 cm
Weight: 60 kg
Family: husband, Gerardo Beni; daughter, Katherine Elizabeth, age 1½ years
Childhood heros: Winston Churchill; Spock on "Star Trek"; the fictional Susan Calvin, the robopsychologist in Asimov's *I, Robot*.
Education: B. Sc., 1976, and Ph.D., 1979, Leicester Polytechnic Institute, England
Patents: seven
Oddest job: walking donkeys
Favorite authors: C.S. Lewis, Philip Dick, Miguel Unamuno
People you most respect: Descartes, Pascal, the Medici, Linus Pauling, Arno Penzias
Favorite food: popcorn, pizza, sushi
Favorite movies: *2001*, *Blade Runner*
Favorite expression: "Take a licking and keep on ticking"
Pet peeves: people who say "it can't be done"
Management credo: hire the best people you can, preferably smarter than you, and set them free
Memberships: the IEEE, American Society for Engineering Education, American Society of Mechanical Engineers
Favorite award: Technology Transfer award at Bell Laboratories
Leisure activities: (since having a child) "What leisure?", (earlier) raising bulldogs, gardening

dent of research for AT&T Co., remarked. "In retrospect, the career steps she made look obvious, but at the time, every step was way ahead of her peers."

Her stubbornness is both a strength and a weakness, Hackwood said, but when she settles on an internal direction, outside influences mean little. Penzias said he was impressed one afternoon at Bell Laboratories when he was standing in the hall talking to a group of company officials and distinguished visitors, and Hackwood came walking by. "She smiled politely and kept moving," Penzias said. "She had to go through there to do her job," and she did not overreact to having to brush past the president of Bell Labs and the chairman of AT&T.

Nor did a lack of ▪ robotics research program at Bell Labs change her direction. Lucky recalled, "She came into my office one day, said 'I want a million dollars and I want to start ▪ robotics effort.' I gave it to her, and she did it. She was gutsy."

She also was not swayed by the fact that, in wanting to be taken seriously, she may have picked one of the toughest fields for a woman. At her first robotics conference, she came close to packing up and getting out. "They had girls in bikinis selling robots," she stated, still amazed. "It was ridiculous."

Just two years in robotics brought what she considers her greatest technical achievement at Bell Labs. Her group of engineers designed and built the labs' first intelligent robot system, which assembled semiconductor devices. They transferred that technology to Western Electric, then the manufacturing arm of the Bell System, where it was used in manufacturing gallium arsenide lasers.

Her current work in robotics at Riverside will have much more impact, she believes, affecting a number of fields. With a 10-person team of graduate students and other professors, she is investigating swarm intelligence and distributed robotic systems. Instead of getting their intelligence from a central computer brain, these robots have little smarts as individuals, but communicate locally and operate intelligently as a collective.

This "society of machines" resembles an ant or bee colony in being ▪ system of nonintelligent drones exhibiting collectively intelligent behavior. Within this area, Hackwood is developing ▪ new field she terms cyborgnetics: the use of simple drone computers as extensions of humans, to be carried like a Walkman or portable telephone and communicating with similar units carried by other humans. Applications range from prison security, riot control, and disaster evacuation systems to intelligent highway control and systems that help to improve the productivity of the handicapped.

SEEKING NEW WORLDS. In 1984, following her promotion to department head, Hackwood faced what she considers her most difficult professional choice: whether to stay at Bell Laboratories or seek her fortunes elsewhere. She felt pulled toward a career in academia by experiences she had in hiring engineers. "I was hiring the best people from the best places, and I found they had no hands-on experience building things," she said. She developed a burning ambition to change the U.S. engineering educational system.

She and three other researchers in her group, including one whom she would later marry, contacted universities around the country, and finally accepted an offer from the University of California at Santa Barbara (UCSB) to come and start a robotics research center.

Building a new research program from scratch was not all scientific glory: Hackwood even found herself starting ▪ bus line to carry students from the main campus to the outside building that housed the laboratory. But dealing with such problems, Hackwood said, is part of the job. "Young people have to understand that you don't have the glory of building the Starship Enterprise without sweating over the wiring diagrams," she said. "You have to do the grunt work to build the big picture."

> "I had no wood, but I had no dead wood, either"

Her research group achieved quite a lot. They built a color vision system for the inspection of very large-scale integrated devices. They used sensory data retrieval and fusion to recreate very small objects three-dimensionally from two-dimensional information. They also made advances in robot hand-eye coordination.

In spite of such successes, in early 1990 Hackwood left UCSB. She had been offered the opportunity of ▪ lifetime—the chance to start a brand new college of engineering. The new state college, at the University of California at Riverside, would be an undertaking that had a blank slate, an opportunity for Hackwood to implement her ideas on engineering education.

As dean, Hackwood would be one of only two female deans of engineering in the United States and the only woman to head an engineering program at ▪ public U.S. university. The state of California, in ▪ time of budget austerity, allocated some US $62 million in start-up costs for equipment and laboratories alone.

Since the last time a college of engineering was started in the United States—a decade ago—much has changed. The cold war is over, the defense buildup is over, and other formerly open fields for electrical engineers are getting crowded.

In setting up the new school, the biggest question Hackwood had to face was, What will the society of the future need the Riverside engineering graduates for?

"Engineering in the future is not going to go into the defense industries," Hackwood said. "It's not going to go as much into aerospace as in the past, and it's not going to expand any more in material science and solid-state device research."

After contacting other educators and industry leaders worldwide, she concluded that the key to the future of engineering is in intelligent systems, using computer technologies to integrate decision-making capabilities and intelligent behavior into all aspects of daily life—from smart credit cards that track bank balances to virtual-reality golf simulators.

She also sees the advent of a new era for environmental engineering, and believes that biomedical engineering will spawn new industries and jobs for the Riverside engineering graduates.

In developing her college program, Hackwood stresses the international nature of engineering. She encourages every engineering student to learn ▪ foreign language and study abroad, and has added Japanese to the college's course offerings.

Hackwood finds building a college similar to engineering in that they both require synthesis, invention, and hard work. Starting from scratch has been both a challenge and a blessing. "I had no wood, but I had no dead wood, either," she said.

When fully developed, the University of California at Riverside's College of Engineering, located in the state's fastest-growing county, will offer undergraduate and graduate degree programs in electrical engineering (the largest speciality), computer science, mechanical engineering, and chemical engineering. It will also have a degree program in environmental engineering, though concern for the environment will be ▪ theme that will cut across all disciplines. The college plans to annually educate some 2000 students with 80 faculty members; currently, 250 students are enrolled. Its first B.S. degrees are scheduled to be awarded in June 1993.

THE MOMMY TRACK? Hackwood has long felt it important to mentor girls aspiring to become engineers. She recruits high school girls to work with her in the summers and takes her students along to international conferences.

"I give a talk at high schools called 'Not a Nerd,'" Hackwood said. "I tell the girls they can get married and have ▪ family and still be engineers." (Hackwood last year gave birth to her first child, who has drastically affected her social life, but not, she feels, her job.)

While her work for the next decade or so seems laid out for her as the new school of engineering grows, Hackwood's career is bound to hold still more surprises.

"With Susan," Bell Labs' Penzias said, "I always expect the unexpected. Never the unreasonable, but definitely the unexpected."

The Smith chart

For half a century, this famous graphical aid has literally run rings around the problems of transmission line analysis

Phillip H. Smith, an engineer at Bell Telephone Laboratories, radically simplified transmission line analysis by developing the graphical aid named after him. He introduced his chart in the 1930s, in time for an enhanced version to prove invaluable to the designers of microwave devices and systems during World War II, and it flourishes to this day, despite being a survivor from an analog age in a digital era.

When Smith invented his chart, analog methods of calculation were everywhere, in the form of slide rules, nomographs, and graphical characteristics of vacuum tubes and electrical machinery. Outliving all the rest, his became perhaps the most distinctive graph in electrical engineering [see illustration] and is still marketed in a variety of forms by the company he founded, Analog Instruments Co.

Smith was born on April 29, 1905, in Lexington, Mass., and majored in electrical engineering at Tufts College in nearby Medford. His alma mater was known for its emphasis on graphic language and especially for the course in engineering graphics taught by Gardner Anthony. Smith graduated from Tufts in 1928 and joined Bell Telephone Laboratories, where he remained until his retirement in 1970.

In 1929 the young engineer was assigned to a short-wave radio transmitting station operated by the Bell Co. in Lawrenceville, N.J. This station employed numerous directive antennas and provided radiotelephone service to both Europe and South America. It was at Lawrenceville that Smith developed his first graphical aid, for matching antennas to transmission lines. He used a rectangular form of a graphical chart based on a transmission line equation credited to the British physicist, John A. Fleming.

Following his transfer, in 1934, to the Radio Development Department at Whippany, N.J., Smith designed phasing and coupling apparatus for a number of commercial broadcasting stations. Meanwhile, he went on improving his transmission line graphs and by 1936 had developed a polar coordinate form on which all values of line impedance could be shown.

Two colleagues showed him how to use a conformal mapping technique to produce a chart with orthogonal circles that were easier to draw than the polar chart. In the conformal mapping chart, the user plots curves of constant standing wave ratio as circles concentric with the chart's center.

Smith disclosed the transmission line calculator in the January 1939 issue of *Electronics*. The paper included a full-page illustration of the chart with a radial arm to be pivoted at the chart center, and described it as suitable for readers to cut out and use as a home-made calculator. Smith published a follow-up article on the chart used as a calculator with improved accuracy in *Electronics* in January 1944. He noted that the war, by then under way, had stimulated interest in the calculator among engineers working in the ultrahigh-frequency field. Researchers working at the Radiation Laboratory at the Massachusetts Institute of Technology in Cambridge were finding that the Smith chart was extremely useful in designing microwave radar systems.

During the war years, Smith himself worked on antennas for the SCR 268, an early radar, and also on microwave radar antennas. After the fighting ended, he developed the so-called cloverleaf antenna for use with frequency modulation broadcast transmitters and received a patent on it in 1950. He also contributed to the design of the antennas for the DEW (distant early warning) line, Nike radar, and SAGE (semiautomatic ground equipment) system in the postwar period.

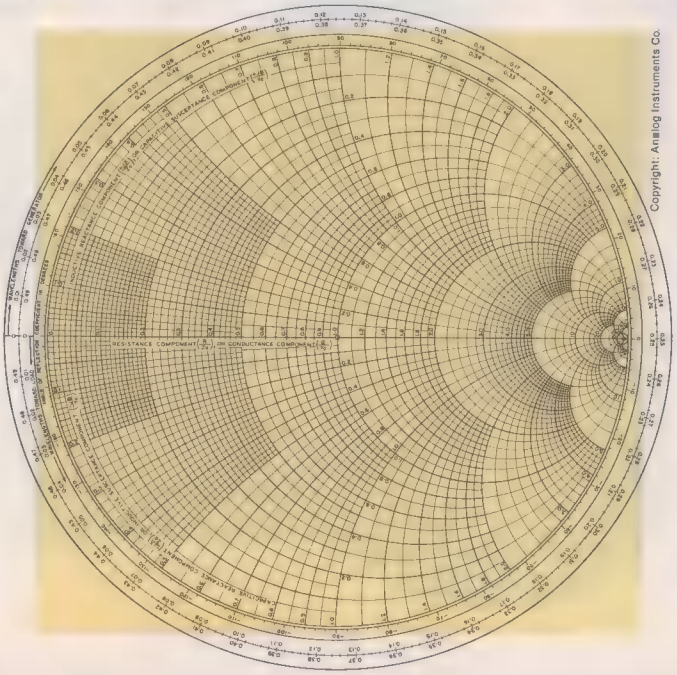
Outside his job, in 1950, Smith turned into a flying enthusiast. He came to own two small airplanes and logged more than 1500 hours in them.

In 1952, he was elected a Fellow of the Institute of Radio Engineers for his contributions to antennas and graphical analysis. In 1969, his book *Electronic Applications of the Smith Chart in Waveguide, Circuit, and Component Analysis* was published.

The next year, he retired from Bell Laboratories and founded Analog Instruments, which sold navigational instruments for the light aircraft he loved, but which later added a line of Smith charts and related items. At the time he died in August 1987, it was reported that more than nine million copies of the chart had been sold.

His wife, Anita M. Smith, has since continued the chart business. The company supplies at least 12 different types of the trademarked Smith chart, including a "negative Smith chart" for the analysis of negative resistance devices. Even modern, computer-based automatic network analyzers rely on the Smith chart for data display, and current textbooks and courses in electrical engineering still feature it.

Furthermore, since 1988 the Smith chart has been cited in papers by engineers in Canada, China, Italy, Singapore, Sweden, the United Kingdom, and the United States in connection with communications, phased arrays, noise parameter measurements, impedance matching, amplifier design, and other topics.



James E. Brittain
Georgia Institute of Technology

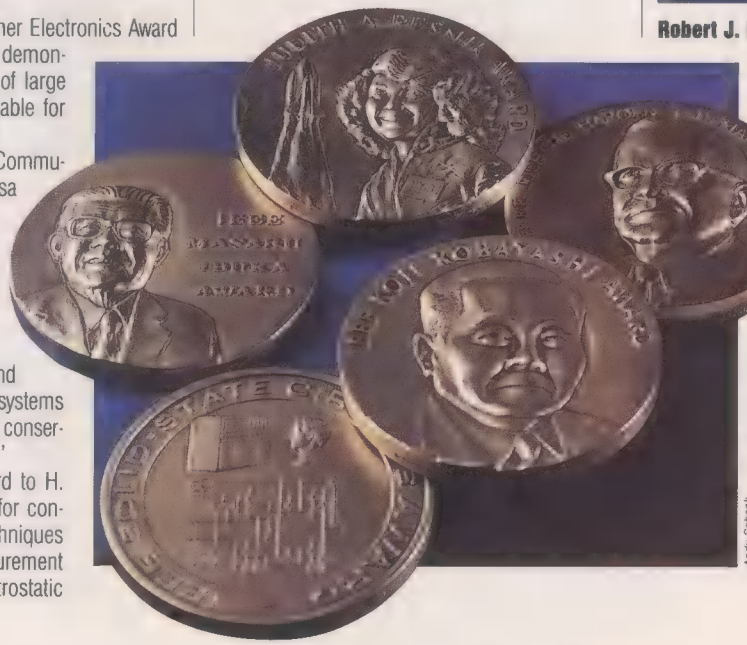
ABOUT THE AUTHOR. James E. Brittain (F) is associate professor at the School of History, Technology, and Society, part of the Georgia Institute of Technology in Atlanta. ◆

IEEE Technical Field Awards

Among the recipients this year are experts in stochastic systems theory, magnetic data storage, and phased-array antennas

The IEEE's annual Technical Field Awards acknowledge outstanding contributions in particular fields of electrical and electronics engineering. This year, the IEEE's Board of Directors chose 22 recipients for 19 awards consisting of certificates, honoraria of up to US $2000, and, in some cases, bronze medals. The 1992 awards and recipients are:

- The Cledo Brunetti Award to David A. Thompson (F) "for pioneering work in miniature magnetic devices for data storage, including the invention, design and development of thin film and magnetoresistive recording heads."
- The Control Systems Award to Harold J. Kushner (F) "for fundamental contributions to stochastic systems theory and its engineering applications."
- The Harry Diamond Memorial Award to Robert J. Mailloux (F) "for contributions and leadership in the development of phased array antennas for radar and communications systems."
- The Herman Halperin Electric Transmission and Distribution Award to Andrew R. Hileman (LF) "for meritorious achievement in the advancement of technology for insulation coordination, switching overvoltages, and testing of high voltage electric power transmission systems."
- The Masaru Ibuka Consumer Electronics Award to Isamu Washizuka (M) "for demonstrating technical feasibility of large size color LCD displays suitable for consumer TV applications."
- The Award in International Communications to Francesco Carassa (LF) "for original contributions in the field of microwave radio relay and satellite communications."
- The Richard Harold Kaufmann Award to Kao Chen (LF) "for technical direction and application of illuminating systems engineering to achieve energy conservation in industrial facilities."
- The Morris E. Leeds Award to H. Kumar Wikramasinghe (F) "for contributions to electrical techniques for nanometer-scale measurement of magnetic, optical, electrostatic and thermal properties of surfaces."
- The Koji Kobayashi Computers and Communications Award to Vinton G. Cerf (F) and Robert E. Kahn (F) "for the creation of the concept of the Transmission Control Protocol/Internet Protocol architecture for packet switched internetting."
- The Morris N. Liebmann Memorial Award to Praveen Chaudhari (nonmember), Jerome J. Cuomo (M), and Richard J. Gambino (M) "for the discovery of amorphous magnetic films used in magneto-optic data storage systems."
- The Jack A. Morton Award to Takuo Sugano (F) "for contributions to metal-insulator-semiconductor device and technology."
- The Frederik Philips Award to Alan G. Chynoweth (F) "for contributions to industrial research management, and fostering the relationship between research, industry, universities and government."
- The Emanuel R. Piore Award to Harold S. Stone (F) "for fundamental contributions to parallel computer technology, and to computer science education."
- The David Sarnoff Award to Jim Hsieh (nonmember) "for the invention and commercialization of the GaInAsP semiconductor laser for fiber-optic communications."
- The Solid-State Circuits Award to Barrie Gilbert (F) "for contributions to non-linear analog signal processing circuits."
- The Charles Proteus Steinmetz Award to Donald C. Fleckenstein (SM) "for leadership in national and international electrical and electronic standardization."
- The Nikola Tesla Award to Thomas H. Barton (F) "for the practical application of the generalized theory of electrical machines to ac and dc drives."
- The Graduate Teaching Award to James H. Mulligan Jr. (LF) "for inspiring graduate students, and leadership in the development of research-based curricula and graduate teaching."
- The Undergraduate Teaching Award to James W. Nilsson (LF) "for motivational teaching, publication of outstanding textbooks, mentoring other faculty, and dedication to his students."



Andy Schenk

David A. Thompson (F, Cledo Brunetti Award) is director of the Advanced Magnetic Recording Laboratory for the IBM Almaden Research Center, San Jose, Calif. He is co-inventor of the magnetoresistive sensor used in all magnetic-bubble memories. The main thrust of his work, however, has been with heads and sensors used for magnetic recording for data storage. In the early 1980s, he helped design the first efficient and manufacturable thin-film recording head for hard-disk drives. He also holds the patent on the shielded magnetoresistive head, which is playing an increasingly important role in advanced tape and disk storage.

Harold J. Kushner (F, Control Systems Award) is professor of applied mathematics at Brown University, Providence, R.I., which he joined in 1964. He has worked in virtually all aspects of stochastic systems analysis and stochastic optimal control. His six books and nearly 140 research papers contain fundamental contributions in these areas. He was one of the originators of the theory of stochastic stability, and his visionary book *Stochastic Stability and Control* was published in 1967.

Robert J. Mailloux (F, Harry Diamond Memorial Award) is chief of the Antennas and Components Division, Rome Air Development Center, L.G. Hanscom Air Force Base in Massachusetts. For the Air Force, he addressed the antenna technology for space-based radars and ground-precision approach radars, receiving patents for a class of antennas called limited-field-of-view systems, which scan electronically over limited sectors of space. Recent research efforts include studies of the sidelobe characteristics of statistically thinned and quantized arrays for large ground-based over-the-horizon radar systems, millimeter-wave phased-array architecture, and the development of algorithms for correcting patterns of arrays with failed elements.

0018-9235/92/$3.00©1992 IEEE

Andrew R. Hileman (LF, Herman Halperin Electric Transmission and Distribution Award) joined Westinghouse Electric Corp., Pittsburgh, in 1951, specializing in the study of insulation coordination. He helped develop models for studying lightning flash and for calculating the lightning flashover rate. As Westinghouse's project leader for the design of the Allegheny Power System's 500-kV lines and stations, he developed switching impulse testing techniques and probabilistic methods of switching surge insulation coordination. In 1989 he left Westinghouse to consult in power systems insulation coordination.

Isamu Washizuka (M, Masaru Ibuka Consumer Electronics Award), with Sharp Corp., Osaka, Japan, for his entire career, was engaged from 1961 to 1985 in researching and developing calculator and personal office equipment, including word processors, personal computers, copiers, and facsimile machines. In 1964 he designed and mass-produced the world's first calculators with transistors. Four years later, he moved on to MOS ICs, and in 1973 began employing dynamic-scattering-mode liquid-crystal displays in the calculators.

Francesco Carassa (LF, Award in International Communications), professor of electrical communications at the Politecnico di Milano, Italy, began his career at the Central Radio Laboratory of Magneti Marelli in Milan in 1947, working on time-division radio systems, microwave propagation, radio relay systems, waveguide communications, and FM television transmission. He helped acquire statistical data on signal propagation and communications in the presence of rain, and evaluated adaptive methods to overcome rain attenuation. An experiment on such a frequency-diversity system is to be carried out soon using the European Olympus satellite.

Kao Chen (LF, Richard Harold Kaufmann Award) spent over 30 years at Westinghouse Electric Corp. and North American Philips Corp. in the design and application of illuminating systems. He developed a relighting program, which was the first to analyze the economic effects of energy and lighting constraints and their effects on worker productivity and satisfaction. Lamp and luminaire engineers applied the data gathered by Chen to make advances in energy-saving lamps, ballasts, and fixtures.

H. Kumar Wickramasinghe (F, Morris E. Leeds Award) is manager, physical measurement, for IBM Corp.'s Thomas J. Watson Research Center, Yorktown Heights, N.Y., which he joined in 1984 to start a group in nondestructive evaluation. He also began his efforts there in scanning probe microscopy. Before joining IBM, he served on the electrical engineering faculty of University College, London, where he and his students pioneered work on acoustic microscopy in gases and ultrasensitive laser differential phase microscopy techniques.

Vinton G. Cerf (F) and **Robert E. Kahn** (F, Koji Kobayashi Computers and Communications Award) are both with the Corporation for National Research Initiatives, Reston, Va. Kahn is president of the not-for-profit organization, which he founded in 1986 following 13 years at the Defense Advanced Research Project Agency (Darpa). Kahn's organization provides leadership and funding for R&D of the U.S. information infrastructure. At Darpa, Kahn initiated the U.S. government's billion-dollar Strategic Computing Program, the largest Federal computer R&D program ever undertaken. Cerf, a vice president of the corporation, manages Internet as well as digital library and electronic messaging research programs. Earlier in his career, he helped develop host communication protocols for Arpanet, and he led a research effort that developed the transmission control and internet protocols (TCP/IP).

Praveen Chaudhari (nonmember), **Jerome J. Cuomo** (M), and **Richard J. Gambino** (M, Morris N. Liebmann Memorial Award) are employed at IBM's Thomas J. Watson Research Center. Chaudhari, now a research staff member, has since 1966 held various management positions, working in such technologies as optical storage, magnetic bubbles, and the Josephson program. He was appointed director in 1981, and from 1982 to 1989 was vice president, science, responsible for science programs at Almaden, Yorktown Heights, and Zurich.

Cuomo is manager of the Materials Laboratory's Advanced Materials Processing area. He joined the center in 1963 and became instrumental in setting up the Material Processing Service Laboratory. Since 1983, Cuomo has managed research projects in enhanced plasma processes, laser deposition, and cathodic arc processes. He is a co-inventor of processes using hollow cathode plasma enhancement, electron cyclotron resonance, inductively coupled plasmas, and collimated sputtering.

At the Watson center since 1961, Gambino researched the magnetic properties of rare-earth alloys and intermetallic compounds as well as thin-film materials for magnetic-bubble devices and magneto-optic storage applications. He is one of the discoverers of perpendicular magnetic anistropy in rare-earth transition metal amorphous-alloy films.

Takuo Sugano (F, Jack A. Morton Award) is dean of the faculty of engineering at the University of Tokyo, which he joined in 1959, and director of the material research group in the Institute of Physical and Chemical Research. He has researched the physics and technology of metal-insulator-semiconductor (MIS) devices, particularly silicon MOS field-effect transistors, and of gallium arsenide and indium phosphide. He has published more than 200 papers and holds numerous patents.

Alan G. Chynoweth (F, Frederik Philips Award), vice president for applied research, Bell Communications Research Inc., Morristown, N.J., since 1983, is responsible for a broad research program for the Bell Operating Companies. The program is heavily oriented toward network operating and software systems while maintaining a foundation in the underlying network hardware technologies.

Harold S. Stone (F, Emanuel R. Piore Award), a research staff member at IBM's Thomas J. Watson Research Center since 1984, has worked on advanced computer architecture and is currently researching cache memory systems and optical interconnections. From 1968 until 1974, while associate professor of electrical engineering and computer science at Stanford University, Stone began studies in the perfect shuffle interconnection pattern and its application to parallel computers. The work on interconnections led to his formulation of the recursive doubling algorithm.

Jim Hsieh (nonmember, David Sarnoff Award) founded Lasertron Inc., Burlington, Mass., in 1980, to develop fiber-optic transmitters and receivers. Lasertron was largely responsible for commercializing indium-gallium arsenide-phosphide (InGaAsP) lasers, which have replaced aluminum-gallium arsenide (AlGaAs) lasers in long-distance communications. At MIT Lincoln Laboratory, Cambridge, Mass., from 1971 to 1980, Hsieh carried out R&D on liquid-phase epitaxy growth of III-V compounds.

Barrie Gilbert (F, Solid-State Circuits Award), manager of the Northwest Laboratories, Analog Devices Inc., Beaverton, Ore., has worked on a wide variety of IC products and processes since joining the company in 1972. He has spent most of his career designing analog circuits, beginning with vacuum tubes in the late 1940s in England, and progressing to superhets, oscilloscopes, and televisions. He helped develop the 7000-series oscilloscope at Tektronix Inc., designed the first ICs for Tektronix, and invented a variety of carrier-domain devices.

Donald C. Fleckenstein (SM, Charles Proteus Steinmetz Award) retired in 1989 as industry standards manager for General Electric Co., Fairfield, Conn. He joined GE in 1950. Throughout his career he served as a member and leader of U.S. and international voluntary standards organizations, including the National Fire Protection Association, the National Electrical Manufacturers Association, and the International Electrotechnical Commission.

Thomas H. Barton (F, Nikola Tesla Award) is emeritus professor of electrical engineering at the University of Calgary, Alta., Canada, where he was dean of the faculty of engineering from 1975 to 1985 following 18 years at McGill University. Professionally, he has focused on electric drives and power electronics. He entered academia in 1951 as a lecturer at the University of Sheffield, England, following two years at the English Electric Co., Stafford, England.

James H. Mulligan Jr. (LF, Graduate Teaching Award) is professor emeritus of electrical engineering at the University of California in Irvine, which he joined as dean in 1974. Previously, he was professor of electrical engineering at New York University and department chairman from 1953 to 1968. His research and teaching interests are in the fields of circuits and systems, with emphasis on electronic circuit applications. He introduced and developed graduate courses in passive and active network theory, including feedback amplifier design; advanced electromagnetic theory; and the design of circuits using discrete and integrated devices.

James W. Nilsson (LF, Undergraduate Teaching Award) is now distinguished professor emeritus in the department of electrical engineering at Iowa State University in Ames, which he joined in 1948. He is the author of *Introduction to Circuits, Instruments and Electronics* (Harcourt, Brace, & World, 1968) and four editions of *Electric Circuits* (Addison-Wesley, 1983, 1986, 1990, and 1993). He coauthored (with R. G. Brown) *Introduction to Linear Systems Analysis* (John Wiley & Sons, 1962). ◆

Books

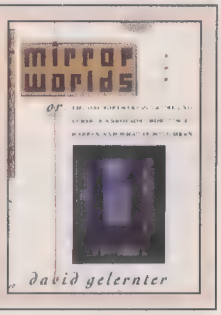
(Continued from p. 12)

ing, but not any more. Now he has fun programming computers at Silicon Graphics Inc., Mountain View, Calif., for audio and video applications. He lives in Silicon Valley with his wife, Sue, his three sons, Benjy, David, and Jonathan, and his Mac, Amiga, and MIDI keyboards.

Brave new [virtual] world

Tom Forester

Mirror Worlds: Or: The Day Software Puts the Universe in a Shoebox . . . How It Will Happen and What It Will Mean.
Gelernter, David. Oxford University Press, New York and Oxford, England, 1991, 256 pages, $24.95 ($12.95 paperback).



Virtual reality, the creation of artificial worlds inside a computer, is the flavor-of-the-month in computing right now. The expected avalanche of books on "cyberspace," "virtuality," and "microcosms" is already under way.

For David Gelernter, a computer science professor at Yale University, New Haven, Conn., the term "mirror worlds" better describes what he sees as a—if not *the*—major feature of computing in the future. Mirror worlds, according to Gelernter, are massively complex software models of some chunk of reality that mimic the real world, second by second, and in every detail.

"You will look into a computer screen and see reality," he writes. "Some part of your world—the town you live in, the company you work for, your school system, the city hospital—will hang there in a sharp color image, abstract but recognizable, moving subtly in a thousand places." Fed by a constant stream of data, the mirror world will be as good as the real thing.

For example, with sufficient complexity, a software model of your city will enable you to check on current traffic conditions, air quality, delays at the airport, the agenda of today's meeting at city hall, the state of the city's finances, prices in the local fruit market, and the current crime rate. By hitting a few keys, the concerned citizen or high-tech tourist will be able to get the full history of any physical features like local parks, or the background to any controversial issue facing the city. The user will even be able to "walk" down the street (having, no doubt, first checked on the whereabouts of well-known muggers) and chat with passers-by.

Further, our user might wish to stop by the local hospital to visit with sick relatives, check on software quality in the patient-monitoring systems, and quiz doctors on the latest treatment methods revealed on the medical databases (which the doctors would undoubtedly appreciate). "The Mirror World isn't a mere information service," Gelernter writes, "it's a *place*." But this place does more than depict reality; it lets users interact with it and intervene in it at will to influence the future course of events: it's the "New Public Square," Gelernter declares.

What's the point of all this? Mirror worlds sound like fun, but so what? To his credit, Gelernter asks himself the same questions early on in this stream-of-consciousness book, but I'm not sure his answers are adequate. His first response is that the mirror world will be a 24-hour-a-day service, which will enable the citizen to access any information he or she needs to understand the workings of today's complex, high-tech society. This sounds fine and democratic, but the sad fact is that the U.S public—through low voter turnout and the failure of various "teledemocracy" experiments—has shown a consistent lack of interest in civic affairs, let alone a burning desire to actually partic-

Circle No. 15

Books

ipate in the political process. I simply cannot see much consumer demand for what will be an extremely expensive software toy, even if it can be constructed.

Second, all the worthy activities Gelernter talks about can just as easily be done in the real world, so why don't we just encourage people to participate more in real politics, business, environmentalism, and so on? Again, Gelernter anticipates this criticism, but his answer hints at a curious, extreme dislike for the quality of life in urban areas of the United States: "For most people, the real world is just too big, sprawling, complicated, disorganized, intimidating, cold-and-wet or smoggy-and-smelly or expensive, unpredictable, inconvenient, dangerous, whatever. . . . It just isn't possible to deal on a friendly basis (on *any* basis) with a whole good-sized town-full of people."

Having betrayed a nerd-like preference for the world inside a cathode-ray tube over a real world of real people, Gelernter somewhat confusingly goes on to extoll the virtues of the idealized small town of U.S. folklore, where "you actually *know* your fellow citizens." Most small communities I have come into contact with have been characterized by long-standing personal animosities and bitter family feuds, which make them anything but idyllic. And anyway, most people like to keep to themselves, and dislike busybodies. Didn't a recent survey show that most people's idea of a good neighbor was someone they never saw?

There are many other apparent contradictions in this book. For example, mirror worlds are variously described as hugely complex and incredibly simple, and the necessary software as almost available and light years away. Much of the detailed technical material is hard to follow and somewhat speculative, to say the least. The author writes well, but there is a lot of repetition and the text could have been better organized and more tightly edited.

In a sense, though, none of this matters because the author is, after all, floating an idea rather than writing a detailed system specification. The notion of mirror worlds can be easily pooh-poohed, and to many computer scientists will seem more science fiction than fact. Yet without such ideas for the future in computing, we will have nothing with which to inspire new generations of students and researchers, and, therefore, no future in computing. We need to compare and contrast such future scenarios as Gelernter's, picking out promising ideas and rejecting the hare-brained.

One thing is certain: thanks to people like Gelernter, there *is* a future of computing and it will be a whole lot different from computing today. One need only go back a decade to realize that amazing advances have occurred. A decade from now we'll wonder how we ever managed with the Stone Age machines of the early 1990s. Mirror worlds probably will not be a reality then, virtual or otherwise, and may never be. But they are an intriguing idea worth considering.

Tom Forester lectures in the social aspects of computing at Griffith University, Queensland, Australia. His books include The Information Technology Revolution *(1985),* The Materials Revolution *(1988),* Computers in the Human Context *(1989), and, with Perry Morrison,* Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing *(1990)—all published in the United States by the MIT Press, 55 Hayward St., Cambridge, Mass., 02142.*

COORDINATOR: Glenn Zorpette

Recent books

Machine Intelligence 12. *Hayes, J.E., et al.,* Oxford University Press, New York, 1991, 342 pp., $120.

Getting Started With Microsoft Word 5.5. *Rampa, Janet,* Microsoft Press, Redmond, Wash., 1991, 399 pp., $22.95.

Forum

(Continued from p. 11)

Brant Rock stations employed rotary spark gap transmitters. The stations were powered by 35-kW steam-engine–driven 125-cycle alternators, with rotary gaps that provided 250 sparks per second.

The antenna systems consisted of tubular towers 36 inches [90 cm] in diameter and 420 feet [130 meters] tall. This power was sufficient to demonstrate that transatlantic communication was possible, using a frequency of about 80 kHz, but insufficient to provide reliable communications. In July 1907 the Machrihanish tower blew down in a storm, and this station was never rebuilt.

In the period between the first trials and the Machrihanish loss, a larger transmitter had been designed and put into construction. This was a 100-kW 500-cycle rotary spark set. It was installed at Brant Rock and gave wonderful results.

The HF alternator used for the 1906 fall and winter telephony tests was a small machine built or rebuilt by Fessenden. It was a Mordey type, having a fixed armature in the form of fixed disk, or ring, and a revolving field magnet with 360 teeth, or projections. At a speed of 222.2 revolutions per second, an alternating current of 80 kHz and a terminal electromagnetic field at 65 volts was generated. The maximum output of the alternator at this speed was about 300 W.

With the Fessenden design, apparently there was very little difficulty in running the machine at so high a speed. A simple flat-belt drive was used, and a thin self-centering shaft that entirely did away with excessive vibration and pressure on the bearings.

J. A. Fleming in his book *Electromagnetic Waves* (published in 1906) said, in reference to Fessenden's patent (No. 706,737, August 1902) for this kind of transmission, that "there was no HF alternator of the kind described by Fessenden, and it is doubtful if any appreciable radiation would result if such a machine were available and used as Fessenden proposes."

Marconi considered that the basis of radio transmission was by way of a "whip-lash" effect, characteristic of the spark gap transmitter, and since he was considered to be the world's expert in radio transmission, no one listened to Fessenden. The progress of radio was retarded a decade by this error. The whip-lash theory passed gradually from the minds of men and was replaced by the continuous wave one, with all too little credit to the man who had been right.

John S. Belrose
Ottawa, Ont., Canada

Too narrow an education

I found Donald Christiansen's "Do students really get it?" [June, p. 19] very interesting. Engineering education is facing many challenges today. The university engineering faculty has become a self-perpetuating group that has lost sight of the purpose of preparing students for an engineering career.

Industry has contributed to the problem by demanding that colleges turn out a product that is immediately useful to them. This has resulted in a narrowly trained engineering graduate who will have no difficulty in adapting to shifts in [a specific] technology, resulting in relatively short careers (about 15 years).

The engineering schools have to return to the concept of turning out engineers well-grounded in the broad basic engineering principles and art. The industrial corporations should train the engineering graduate in the specialties (one to three months) for their specific needs.

The present over-emphasis on computer science is an example of this narrow training, where industry is becoming saturated with computer engineers, but needs other engineering specialties. The computer science engineer has not been exposed to analog circuitry, power distribution systems, radio/radar, mechanical devices, hydraulics, and so on, which would allow transfer to other areas of engineering.

Walter W. Frey
Swanton, Vt.

Corrections

On p. 17 of the June issue, second column, first and fourth lines, the patent numbers should have been 5011254 and 4932989.

On p. 27 of the July issue, the labels "Floating-point pipeline and registers" and "Branch cache" should have been transposed, and the label "Data cache" should have been moved up closer to the blue lines on the chip.

On p. 55 of the July issue, the photos of two medalists were transposed. The photo of Charles Elachi, awarded the IEEE Medal for Engineering Excellence, was transposed with the photo of James L. Massey, awarded the IEEE Alexander Graham Bell Medal.

—Ed.

Readers are invited to comment in this department on material previously published in *IEEE Spectrum*; on the policies and operations of the IEEE; and on technical, economic, or social matters of interest to the electrical and electronics engineering profession. Short, concise letters are preferred. The Editor reserves the right to limit debate on controversial issues. Contacts: Forum, *IEEE Spectrum*, 345 E. 47th St., New York, N.Y. 10017, U.S.A.; fax, 212-705-7453. The Compmail address is ieeespectrum. The computer bulletin board number is 212-705-7308 and the password is SPECTRUM; for more information, call 212-705-7305 and ask for the Author's Guide.

PRODUCT PROFILES

The PRODUCT PROFILES advertising section provides a distinctive focus on both new and commercially established products and services that offer practical solutions for engineering and scientific professionals in today's fast-paced, rapidly changing high-tech environment.

R&M PREDICTION AND FMECA SOFTWARE

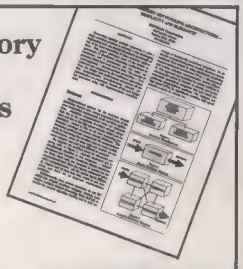
Powertronic Systems offers software to predict reliability, maintainability and FMECA. Since 1982, hundreds of users have selected from our large, versatile, integrated software family for military and industrial equipment, electrical or mechanical. Program highlights include: visible assembly hierarchy, defaults and library data, extensive report sorting, user defined reports, what-if and derating analysis, and concurrent engineering data links.

- MIL-HDBK-217
- MIL-HDBK-472
- MIL-HDBK-338
- Bellcore
- DTRC-90/010
- MIL-STD-1629
- MIL-STD-756B
- NPRD-91

POWERTRONIC SYSTEMS, INC.
13700 Chef Menteur Hwy.
New Orleans, LA 70129
504-254-0383 • FAX: 504-254-0393

Circle No. 51

Shared-Memory Networking Architectures Technical Paper



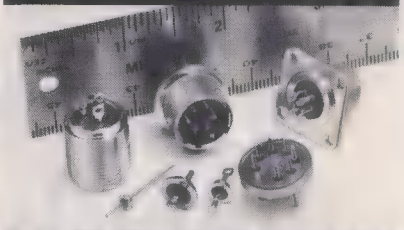
The unique requirements of distributed computing architectures for real-time applications, such as aircraft simulators, are addressed in this 8 page paper. It examines the major approaches used to date and introduces the new concept of shared-memory networking. Design and performance parameters of the first such network are explored, along with implementation considerations. Request **free** copy. **Systran Corp.**, 4126 Linden Avenue, Dayton, OH 45432-3068 USA. Phone (513) 252-5601 or 1-800-252-5601; Fax (513) 258-2729.

Circle No. 52

HERMETICALLY SEALED

Mini Connectors, Headers and Terminals

Pressure and Vacuum Types



DETORONICS
10660 E. Rush St. • So. El Monte, CA 91733-3432
Phone (818) 579-7130 • FAX (818) 579-1936
Let us quote your requirements. Simply send [illegible] or give us a call.

Circle No. 53

Relex RELIABILITY SOFTWARE

"The Intuitive Solution!"

Analyze and improve your product reliability using this advanced, state-of-the-art set of software tools.

Relex products are noted for their outstanding quality, ease-of-use, flexibility, and comprehensive array of features. A wide range of packages are available to meet your product requirements. And all Relex products fully guaranteed!

- ★ Reliability Prediction
  - MIL-HDBK-217
  - Bellcore
  - French CNET
  - Parts Count
- ★ FMECA
- ★ Maintainability
- ★ Fault Tree
- ★ Thermal
- ★ Weibull
- ★ more ...

Call 410-788-9000 Today For More Information!

[illegible] Systems Division, Inc.
Two English Elm Court • Baltimore, MD 21228 USA
410-788-9000 • FAX 410-788-9001

Circle No. 54

Your Ad Here!

YOUR HEADLINE

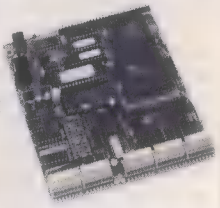
This area may be used by advertisers to detail their ad message in 50 words or less. Just provide typed copy with appropriate direction for emphasis (bold, underscore, etc.), we'll do the rest. Be sure to include repros of your company logo, etc. Indicate if you wish us to set addresses, phone #, etc. For rates and production information, phone 212-705-7579.

COMPANY NAME/LOGO HERE
Mailing Address/Phone

AD SIZE: 2⅛" × 3"

MICROCONTROLLERS

- C Programmable
- Data Acquisition
- Control / Test
- Excellent Support
- From $159 Qty 1
- *New* Keyboard Display Modules



Use our **Little Giant**™ and **Tiny Giant**™ miniature controllers to computerize your product, plant or test department. Features built-in power supply, digital I/O to 48+ lines, serial I/O (RS232 / RS485), A/D converters to 20 bits, solenoid drivers, time of day clock, battery backed memory, watchdog, field wiring connectors, up to 8 X 40 LCD with graphics, and more! Our $195 interactive **Dynamic C**™ makes serious software development easy. You're only *one* phone call away from a total solution.

Z-World Engineering
1724 Picasso Ave., Davis, CA 95616
(916) 757-3737 Fax: (916) 753-5141
Automatic Fax: (916) 753-0618
(Call from **your fax**, request catalog #18)

Circle No. 55

Employment opportunities

Organizations seeking engineers and scientists describe their various openings in the following advertising section In order to conform to the Age Discrimination in Employment Act and to discourage age discrimination, IEEE may reject any advertisement containing any of these phrases or similar ones, "recent college grads," "1–4 years maximum experience," "up to 5 years experience," or "10 years maximum experience." IEEE reserves the right to append to any advertisement, without specific notice to the advertiser, "Experience ranges are suggested minimum requirements, not maximums." IEEE assumes that, since advertisers have been notified of this policy in advance, they agree that any experience requirements, whether stated as ranges or otherwise, will be construed by the reader as minium requirements only. While IEEE does not ban the use of the term "entry level," its use is discouraged since, to some, it connotes an age rather than an experience designation. IEEE accepts employment advertising to apprise its members of opportunities. Interested parties should be aware that the political and humanistic values of certain advertisers may differ from their own. IEEE encourages employers to offer salaries that are competitive, but occasionally a salary may be offered that is significantly below currently acceptable levels. In such cases the reader may wish to inquire of the employer whether extenuating circumstances apply.

To place an advertisement in *Spectrum*'s Employment Opportunities section, contact the nearest *Spectrum* sales office

New York	Boston	Chicago	San Francisco	Los Angeles	Atlanta	Dallas
212-705-7760	508-255-4014	708-446-1444	415-386-5202	310-649-3800	404-256-3800	214-553-9896

For production/mechanical information contact Theresa Fitzpatrick Advertising Production Manager, 212-705-7579

IEEE Spectrum Advertising Dept., 345 E. 47th St., New York, N.Y. 10017

Photo Courtesy of Boulder Convention & Visitors Bureau

A View to the Future!

Reach new career heights at Bandgap. . . As a result of rapid expansion, BANDGAP TECHNOLOGY CORPORATION, the leader in vertical cavity surface emitting laser arrays, has the following openings for key personnel at its state-of-the-art facility near Boulder, CO:

Manager, Photonics Packaging and QA

Responsible for the packaging, reliability testing and final quality assurance of photonic devices, primarily surface emitting laser arrays. Will manage technicians and engineers in the characterization and quality assurance of the packaging and testing of photonic devices. Responsibilities will include the packaging, test, and final quality control, as well as intensive contacts with customers and industry groups. Will provide leadership in contracted program activities. The ideal candidate will have a M.S. or Ph.D. in E.E., and/or mechanical engineering, management experience, a strong industrial background in the packaging of optical components, and substantial exposure to Production Control, QA/QC and SPC programs. Respond to Dept. 7.

Supervisor, Process Development

Responsible for developing, evaluating, characterizing and optimizing new III-V semiconductor microelectronic and microphotonic fabrication processes for emerging optoelectronic products. Will advise and supervise process development engineers in the development of new implantation, etching, photolithography and deposition processes. This position requires interaction with customers and industrial partners and support of existing and future contracted program activities. The ideal candidate will have a M.S. or Ph.D in E.E., materials science, previous management experience, and a successful industrial background in III-V semiconductor process design. Respond to Dept. 8.

Supervisor, Photonics Design

Responsible for the planning and development of optical, electronic and photonic devices and subsystems. Will supervise designers in the development of a new generation of photonic components. This position requires interaction with customers and industrial partners and support of existing and future contracted program activities. The ideal candidate will have a Ph.D. in E.E., optics, or physics, previous management experience, and an industrial background in the design management of optical, electronic and/or photonic components. Excellent communication skills are essential. Respond to Dept. 9.

Supervisor, Device Test

Responsible for the testing of electronic and photonic devices. Will supervise engineers and technicians engaged in optical and electronic testing of devices. Will develop electronic and photonic testing techniques and algorithms. This position requires contact with customers and industrial partners, and assisting with contracted program activities. The ideal candidate will have a M.S. or Ph.D. in E.E., or physics, previous management experience, and a successful industrial background in III-V semiconductor process design. Excellent communications skills are essential. Respond to Dept. 10.

Circuit/System Design Engineer

This employee will design and test electronics to interface with new photonic devices and optoelectronic subsystems. Will interact with device design, packaging and marketing personnel to introduce new products. Responsibilities include design, simulation and test of digital and analog interface electronics for optoelectronic subsystems. The ideal candidate will have a M.S. or Ph.D. in E.E., a record of successful industrial circuit design in Si and/or GaAs technologies, and past experience with laser driver and photodetector electronics. Respond to Dept. 11.

Software Engineer

This employee will adapt industrial control, communications, simulation and modeling, automated test and business computer software for applications within the Bandgap organization. Will interact closely with epitaxial growth, design, administration, characterization and test personnel to modify existing software, and to implement additional computer capabilities in these areas. Candidates will have a B.S. or M.S. in E.E., mechanical or chemical engineering, experience in writing, documenting and adapting PC and HP-based computer control, test and monitoring software for general application. Respond to Dept. 12.

As a resident of Boulder, you will find a scenic Rocky Mountain view, and numerous recreational activities and cultural events just minutes away. Consider Bandgap. We offer excellent benefits and compensation commensurate with experience. Send resume, cover letter with salary history and corresponding department number to: **BANDGAP TECHNOLOGY CORPORATION, Attn. Ms. Andrea Reale, 325 Interlocken Parkway, Broomfield, CO 80021.** Equal Opportunity Employer.

BANDGAP
Technology Corporation

Calendar

(Continued from p. 14D)

International Symposium on Time-Frequency and Time-Scale Analysis (SP); Oct. 4–6; Victoria Conference Center, Victoria, B.C., Canada; Jan Kvamme, Engineering Continuing Education, University of Washington, 4725 30th Ave., N.E., Seattle, Wash. 98105; 206-543-5539; fax, 206-543-2352.

GaAs Integrated Circuits Symposium (ED); Oct. 4–7; Fontainebleau Hilton Hotel, Miami Beach, Fla.; Suzanne Kuntz, Courtesy Associates, 655 15th St., N.W., Suite 300, Washington, D.C. 20005; 202-347-5900; fax, 202-347-6109.

International Telecommunications Energy Conference (PEL, COM); Oct. 4–8; J.W. Marriott Hotel, Washington, D.C.; Pete Paradissis, Reliance Telecommunications, 1122 F St., Lorain, Ohio 44052; 216-288-1122.

Bipolar/BiCMOS Circuits and Technology Meeting (ED); Oct. 5–6; Marriott City Center Hotel, Minneapolis, Minn.; John Shier, VTC Inc., 2800 East Old Shakopee, Bloomington, Minn. 55425; 612-853-3292; fax, 612-853-3355.

11th Symposium on Reliable Distributed Systems (C); Oct. 5–7; Windham Warwick Hotel, Houston, Texas; IEEE Computer Society, Conference Department, 1730 Massachusetts Ave., N.W., Washington, D.C. 20036-1903; 202-371-1013; fax, 202-728-0884.

Digital Avionics Systems Conference (AES, Seattle); Oct. 5–8; Westin Hotel, Seattle, Wash.; Jose Bolanos, Boeing, M/S 96-16, Box 3707, Seattle, Wash. 98124; 206-237-3719; fax, 206-237-6088.

International SOI Conference (ED); Oct. 6–8; Marriott at Sawgrass Resort, Ponte Vedra, Fla.; Jerry Brandewie, Sematech (Rockwell International), 2706 Monpopolis Dr., Austin, Texas 78741; 512-356-3449; fax, 512-356-3521.

International Conference on Computer Design: VLSI in Computers and Processors—ICCD '92 (ED); Oct. 11–14; Royal Sonesta Hotel, Cambridge, Mass.; IEEE Computer Society, 1730 Massachusetts Ave., N.W., Washington, D.C. 20036-1903; 202-371-1013.

Military Communications Conference (COM); Oct. 11–14; Sheraton Harbour Island Hotel, San Diego, Calif.; John Peckham, General Dynamics Corp., Box 85468, San Diego, Calif. 92138; 619-573-5452; fax, 619-592-5320.

Calendar

International Symposium on Systems, Man and Cybernetics (SMC); Oct. 18–21; Knickerbocker Hotel, Chicago; Richard Saeks, Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, Ill. 60616; 312-567-3221.

Sixth Annual Leesburg Workshop on Concurrent Engineering (R); Oct. 19–22; Xerox Training Center, Leesburg, Va.; Henry N. Hartt, Vitro Corp., Suite 300, West Wing, 600 Maryland Ave., S.W., Washington, D.C. 20024; 202-646-6339; fax, 202-646-6398.

Visualization '92 (C); Oct. 19–23; Boston Park Plaza Hotel, Boston; IEEE Computer Society, Conference Department, 1730 Massachusetts Ave., N.W., Washington, D.C. 20036-1903; 202-371-1013; fax, 202-728-0884.

Workshop on Power Electronics in Transportation (PEL); Oct. 22–23; Hyatt Regency Hotel, Dearborn, Mich.; V. Anand Sankaran, Ford Motor Co., Room S-2037, Scientific Research Laboratory, 20 000 Rotunda Dr., Dearborn, Mich. 48121-2053; 313-390-8689.

Wafer Level Reliability Workshop (ED); Oct. 25–28; Stanford Sierra Lodge, Lake Tahoe, Calif.; Harry Schaft, National Institute of Standards and Technology, Building 225, Room B360, Route 270, Quince Orchard Road, Gaithersburg, Md. 20899; 301-975-2234; fax, 301-948-4081.

26th Annual Asilomar Conference on Signals, Systems, and Computers (SP, C); Oct. 26–28; Asilomar Hotel, Pacific Grove, Calif.; James A. Ritcey, Department of Electrical Engineering, FT-10, University of Washington, Seattle, Wash. 98195; 206-543-4702; fax, 206-543-3842.

NOVEMBER

Regional Symposium on Electromagnetic Compatibility (EMC, Region 8); Nov. 2–5; Tel Aviv Hilton Hotel, Israel; Symposium Secretariate, Ortra Ltd., Box 50432, Tel Aviv 61500, Israel; Dani Tider, (972+3) 664 825; fax, (972+3) 660 952.

International Conference on Computer-Aided Design (ED); Nov. 9–12; Santa Clara Convention Center, Santa Clara, Calif.; IEEE Computer Society, 1730 Massachusetts Ave., Washington, D.C. 20036-1903; 202-371-1013; fax, 202-728-0884.

Technologies Enabling Tomorrow (C et al.); Nov. 11–13; World Congress Center,

(Continued on p. 70H)

INFINITE CHALLENGES

E-Systems ECI Division is in need of engineers with military satellite communication experience (ground, manpack/man-portable, airborne, or spaceborne); a BSEE/BSCE; and at least 2 years' experience in one of the following areas:

SOFTWARE

- ADA, C
- 1750A, of 68020 Microprocessors
- VAX VMS, Sun UNIX
- Real-time, Embedded Microprocessor
- DOD-STD-2167A, CASE Tool

DIGITAL HARDWARE

- ACTEL FPGAs
- Microprocessor based systems
- 1553 bus interface

DIGITAL SIGNAL PROCESSING

- Discrete Fourier Transforms
- Control Loops
- PSK Demodulation

EMBEDDED CRYPTO

- Security Fault Analysis
- TEMPEST, Red/Black Isolation
- Related interface hardware

RF and MICROWAVE

- Synthesizer Design, Direct Digital
- Power amp and filter design
- MMIC design

ANTENNA DESIGN

- Parabolic Antenna Design
- Gimbal, Positioner
- 10 TO 60 GHz

SYSTEMS

- BSEE/MSEE, minimum 4 years' experience
- Strong communication background
- Requirements Analysis, Functional Analysis
- System Synthesis, System Analysis
- RF Link Budget Analysis
- System Integration/Test
- Customer Interface

Background: Hardware, Software Architecture Cryptographic; BIT/BITE; Antenna Pointing, Tracking, and Platform Stabilization; MIL-STD-1582; SI-1135, SI-2035, LL1005.

MILSTAR or other military satellite design experience a plus.

E-Systems offers very competitive salaries and an excellent benefits package which includes an Employee Stock Ownership Plan, 401(k), and major medical and dental insurance. Qualified candidates should forward a resume and salary history to: Manager of Staffing, E-Systems, Inc., ECI Division, Post Office Box 12248, St. Petersburg, Florida 33733-2248.

E-SYSTEMS
The science of systems

U.S. Citizenship Required.
An Equal Opportunity Employer, M/F, D,V.

KUWAIT INSTITUTE FOR SCIENTIFIC RESEARCH

Kuwait Institute for Scientific Research (KISR) is a nonprofit organization actively engaged in applied research in the fields of environmental and earth sciences; food resources; engineering; petroleum, petrochemcials and materials and techno-ecomonics.

KISR has a vacancy in the following field:

ELECTRICAL POWER SYSTEM

Major duties:

- Planning and analysing of power generation and transmission system and modelling techniques under steady and dynamic state.
- Identifying research areas in power system relevant to Kuwait.
- Developing research proposals and carrying out research projects that address problems relevant to Kuwait.
- Developing research and technical capabilities of existing staff in the area of power systems.

Qualifications:

Applicants should have a Ph.D. in Electrical Power System plus at least 12 years of relevant experience with good publication record.

KISR offers attractive tax free salaries commensurate with qualifications and experience and generous benefits that include: gratuity, free furnished airconditioned accommodation, school tuition fees for children, six weeks annual paid vacation, air tickets, free medical care and life insurance.

Interested applicants are requested to send their Curriculum Vitae with supporting information not later than one month from the date of this publication, to:

Personnel Manager
Kuwait Institute for Scientific Research
P.O. Box 24885
13109 Safat - Kuwait

EPRI's Mission is...

...to discover, develop, and deliver advances in science and technology for the benefit of our member electric utilities, their customers, and society.

Project Manager -

Power Systems Planning & Operations

Make a valuable contribution in our power systems planning and operations program by managing multiple power projects in power system planning, flexible AC transmission system, and power system analysis. A proven professional with the ability to monitor contractor performance and manage project budget will be needed.

We want to interview with candidates who possess a BSEE (MSEE or MBA preferred), 6-8 years of experience in the electric utility industry, or a vendor organization with a primary focus in the areas of power system planning, power system dynamic/reliability performance, transmission resource and energy transaction analysis.

Demonstrated knowledge/expertise in the application of power system analysis software, such as power flow and stability, system reliability evaluation, and transmission planning techniques will be required. Excellent verbal and written communication skills a must for this position within our Palo Alto headquarters.

EPRI is a unique non-profit, R&D organization offering a competitive salary, generous relocation program and excellent benefits. Please submit your resume and salary requirements to: **EPRI, Human Resources, Dept DM-MPSA-IEEE, 3412 Hillview Avenue, Palo Alto, CA 94303.** An Equal Opportunity Employer.

EPRI
Electric Power Research Institute

Leadership in Science and Technology

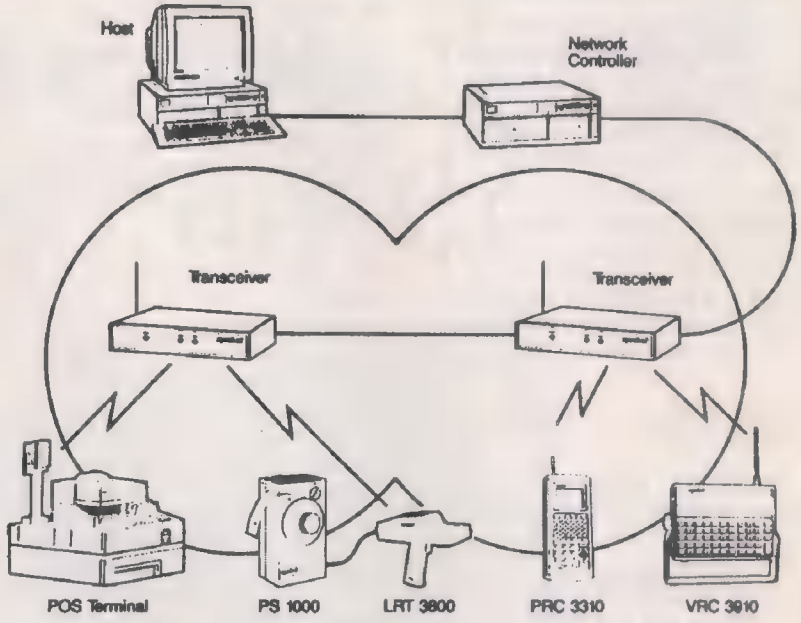
THE FUTURE IS WIRELESS.

THE TECHNOLOGY IS symbol®

TECHNOLOGIES, INC.

While everyone has been talking about wireless computer networks, we have been designing, manufacturing and selling them. Symbol has already installed over 1,500 Spectrum One wireless cellular networks. Symbol Spectrum One Network gives Symbol's hand held computer wireless access to the user's host computer for applications in the retail, transportation and warehousing industries.

At Symbol Technologies, Inc.'s San Jose RF Design Center, you will join an innovative team of Engineers involved in RF circuit design, digital communications research, RF and LAN protocol and software development. Your ideas will become reality in our next generation of wireless networks.



PRINCIPAL ENGINEER - RF DESIGN

You must possess a BSEE (MSEE preferred), coupled with 15+ years of relevant RF design experience primarily in the 1 to 3 Ghz frequency range. Additional experience in complete radio design, including receiver planning and design; up-converter, synthesizer, and power amp design; and design for low cost, high volume manufacturing is required. Familiarity with RF CAD tools is essential. A thorough understanding of modulation theory for digital communications is a plus.

COMMUNICATION TECHNOLOGIST

You must possess an MSEE (Ph.D. preferred), coupled with expertise in modulation theory for digital communications. A strong background in coding theory and familiarity with signal processing CAD and packet based local and wide area networks is essential. Experience with spread spectrum techniques and some commercial industry experience is a plus.

Symbol Technologies, Inc. offers a competitive salary and benefits package. For immediate consideration, please send your resume to **Symbol Technologies, Inc., Attn: Human Resources Department PE/CT, 340 Fischer Ave., Costa Mesa, CA 92626.** Equal Opportunity Employer M/F/V/H. Principals Only Please.

Calendar

(Continued from p. 70E)

Melbourne, Australia; Marg Scarlett, Convention Network, 224 Rouse St., Port Melbourne, Victoria 3207, Australia; (61+3) 646 4122; fax, (61+3) 646 7737.

Second Workshop on the Management of Replicated Data (C); Nov. 12–13; Monterey Marriott Hotel, Monterey, Calif.; Jehan-François Paris, Department of Computer Science, University of Houston, Houston, Texas 77204-3475; 713-749-3943; fax, 713-749-2378.

New Generation Knowledge Engineering (C); Nov. 16–18; Doubletree Washington National Airport Hotel; Julie Walker, 11820 Parklawn Dr., Rockville, Md. 20852-2529; fax, 301-231-7826.

LEOS '92 Annual Meeting (LEO); Nov. 16–19; Hynes Convention Center, Boston; IEEE/LEOS, 445 Hoes Lane, Box 1331, Piscataway, N.J. 08855-1331; 908-562-3896.

International Conference on Communication Systems/International Symposium on Information Theory and Its Applications—ICCS/ISITA '92 (IT, COM); Nov. 16–20; Westin Stamford and Westin Plaza Hotels, Singapore; Esther Yeo, Mansfield International, 71 Robinson Rd., 4th Storey, Crosby House, 0106, Singapore; (65) 224 0000.

Wescon '92 (Region 6, Los Angeles Council); Nov. 17–19; Anaheim Convention Center, Anaheim, Calif.; Electronic Conventions Management, 8110 Airport Blvd., Los Angeles, Calif. 90045; 213-215-3976 or 800-877-2668.

18th Annual Convention and Exhibition (ACE '92) (Calcutta, India C); Nov. 21–23; Birla Industrial and Technological Museum, Calcutta, India; Secretariat, c/o Department of E&T.C.E., Jadavpur University, Calcutta-700 032, India; (91+72) 2851; telex, (91) 0215195.

First Asian Test Symposium (C); Nov. 26–27; Hiroshima Grand Hotel, Hiroshima, Japan; IEEE Computer Society, Conference Department, 1730 Massachusetts Ave., N.W., Washington, D.C. 20036-1903; 202-371-1013; fax, 202-728-0884.

DECEMBER

37th Annual Conference on Magnetism and Magnetic Materials (MAG); Dec. 1–4; Westin Galleria Hotel, Houston, Texas; Diane Suiters, Courtesy Associates, 655 15th St., N.W., Suite 300, Washington, D.C. 20005; 202-639-5088.

Was This The Last Time You Bought Insurance?

Face it—it's been a long time. A lot has changed since then. Your family. Maybe your job. And more than likely, the amount and types of coverage you need from your insurance program. That's why you need insurance that can easily adapt to the way your life changes—Group Insurance Program for IEEE Members.

We Understand You.

Finding an insurance program that's right for you isn't easy. But as a member of IEEE, you don't have to go through the difficult and time consuming task of looking for the right plans—we've done that work for you. What's more, you can be sure the program is constantly being evaluated to better meet the needs of our members.

We're Flexible.

Updating your insurance doesn't have to be a hassle. With our plans, as your needs change, so can your coverage. Insurance through your association is designed to grow with you—it even moves with you when you change jobs.

We're Affordable.

What good would all these benefits be if no one could afford them? That's why we offer members the additional benefit of reasonable rates, negotiated using our group purchasing power. Call 1 800 424-9883 (in Washington, DC, (202) 457-6820) between 8:30 a.m. and 5:30 p.m. Eastern Time for more information about these insurance plans offered through IEEE:

Term Life ▪ Disability Income Protection ▪ Comprehensive HealthCare • Excess Major Medical ▪ In-Hospital ▪ High-Limit Accident • Long Term Care ▪ Medicare Supplement ▪ Cancer Expense

Group Insurance Program for IEEE Members

Designed for the way you live today.
And tomorrow.

EEs' tools & toys

Graphing calculators show it our way

Two new programmable scientific calculators from Sharp are a pleasure to use because they allow equations to be entered, viewed, and edited the way we like to see them: they show exponents as superscripts, and as the photo makes clear, display integral's limits of integration in their traditional positions at the ends of the integral symbol. (The norm is to use the exp function for exponents, and to enter integration limits in ways that lack any visual connection with the integral, separating them with commas or other means.)

Both the EL-9200 and EL-9300 employ an efficient menu system for fast access to a variety of functions. To simplify operation, four direct-access keys allow instantaneous switching among the calculators' main modes: graphing, statistics, programming, and calculating. With this feature, user may interrupt a graphing operation, for example, to do a quick computation, then return to the graph, and pick up where she left off.

The calculators can display four of 99 stored equations at time, graphing them in a choice of rectangular, polar, or parametric coordinates. For clarity's sake, they handle statistical data in a "card" format, with one data set or observation per card. Statistical data can be displayed in seven graph formats.

Up to 99 Basic-like programs may be stored. They may include subroutines, conditional and unconditional branching, and interaction with the calculators' graphing, statistics, and matrix features.

In addition, the EL-9300 has an equation solver; a communications port for connecting the calculator to an overhead projector (EL-92T), another calculator, or a printer (CE-50); and lithium backup battery to retain stored data while changing the main battery (four AAA cells). It also has 32K bytes of RAM compared with the EL-9200's 8K bytes.

Errors are less likely when a calculator displays equations in the traditional manner; for example, with the limits of integration indicated at the ends of the integral symbol.

The EL-9200 and -9300 have suggested retail prices of US $119.99 and $149.99, respectively. The EL-92T overhead projector is $399.99. *Contact: Sharp Electronics Corp., Sharp Plaza, Mahwah, N.J. 07430; 800-BE-SHARP; or* **circle 106.**

CONSUMER

PC software simulates SLR cameras

Kodak PCphotographer is a program that simulates a 35-mm single-lens reflex (SLR) camera on an IBM-compatible personal computer. With it, a user selects a scene, a film type, and a camera position, and then sees how different camera settings affect the final picture.

The program has beginner and advanced modes, suiting both novices and advanced amateurs. It can handle fixed and zoom lenses, flash units, and even spot meters. The simulated photographs it produces let photographers see the effects of bracketing, changes in depth of field, motion, over- or underexposure, focusing, and so on.

Besides the program, the PCphotographer package includes 64-page user's manual, a database of information on Kodak film and filters, an on-line reference on photography in general, and an 80-page photo workshop book. It lists for under US $60.

The software will run on any IBM-compatible PC with 640K bytes of RAM and either a Hercules monochrome graphics card or an EGA or VGA color graphics card. Best performance will be obtained with 286-based computers and better.

The package will be distributed through photo retailers and computer software outlets. *Contact: Eastman Kodak Co., 343 State St., Rochester, N.Y. 14650-0519; 800-242-2424, ext. 67; or* **circle 107.**

INSTRUMENTATION

Boundary-scan test freebies

Heard of boundary-scan testing but not sure whether it's for you? Then two free pieces of literature from Fluke might help. The first, "The ABCs of Boundary-Scan Test," is 44-page introduction to the technology. Although it starts with the basics, the booklet gives quite a bit of detail on IEEE Standard 1149.1, which prescribes an overall test architecture and a set of standard commands.

As the booklet points out, boundary-scan testing was conceived to overcome problems in testing densely populated boards that were difficult or impossible to probe with bed-of-nails fixtures. But users have found that, in addition, it speeds product development, reduces production test setup time, and slashes test-equipment costs.

The other freebie is a poster-sized sheet, "Boundary-Scan: An Integrated Strategy," that details a boundary-scan test feasibility study at Philips International BV. Its many diagrams clarify many testing details.

Contact: John Fluke Manufacturing Co., Box 9090, Everett, Wash. 98206; 800-44-FLUKE. Within Europe, Philips Test and Measurement, Building TQ III-4, 5600 MD Eindhoven, the Netherlands; or **circle 108.**

Where microwave measurement is at

Anyone involved in making precision microwave measurements will appreciate a paper that appeared in special May 1992 issue of *Metrologia*, which is published by the Bureau International des Poides et Mesures (the International Bureau of Weights and Measures) in Paris. Prepared by the National Institute of Standards and Technology (NIST) in Boulder, Colo., the paper summarizes the principles and present status of microwave measurements in scattering parameters, noise, and power.

Among the topics covered are calibration methods for automatic network analyzers, on-wafer monolithic microwave IC (MMIC) measurements, radiometric techniques for measuring noise, and the use of microcalorimeters and other high-accuracy techniques for measuring power. The paper also contains an extensive bibliography. Oh, and everything is in English. *Contact: Jo Emery, Division 104, National Institute of Standards and Technology, Boulder, Colo. 80303; 303-497-3237 (ask for paper 25-92).*

EDUCATION

An English voice from Japan

Original papers on Japanese research in electronics, as well as papers invited from outside Japan, appear in English in *IEICE Transactions*—four publications of Japan's Institute of Electronics, Information and Communications Engineers in Tokyo. The publications also feature tutorials and articles on "hot topics," as an advertisement for the magazines described them—all of which are written in English expressly for the *IEICE Transactions*. With 39 000 members, the institute is Japan's largest engineering society.

In the past, the English-language *IEICE Transactions* was single publication. This

year, for the first time, it has been divided into four monthly volumes: *Fundamentals of Electronics, Communications, and Computer Science*; *Communications*; *Electronics*; and *Information and Systems*. The annual subscription fee for each volume (12 issues) is US $100; a 10 percent discount is offered for subscribers to all four volumes, lowering the cost of 48 issues to $360. *Contact: Maruzen Co., International Division, Export Department, Box 5050, Tokyo International 100-31, Japan; or* **circle 109.**

SOFTWARE

DSP add-ons for Mathcad 3.1

A collection of more than 60 digital signal-processing functions have been gathered together to make up the first of a planned series of add-on Function Packs for use with Mathcad 3.1, the popular technical calculation system. Among the capabilities included in the new pack are transform analysis, spectral analysis, time series analysis, digital filtering, and filter design.

Upon installation, the Signal Processing Function Pack becomes integrated with Mathcad's built-in function set. The added functions are used in the same way as all other Mathcad functions.

Versions of Mathcad are obtainable for PCs, Apple Macintoshes, and Unix workstations. So far, the program has been produced in four languages besides English: German, French, Italian, and Japanese.

The Signal Processing Function Pack is priced at $249. It is available now. *Contact: MathSoft Inc., 201 Broadway, Cambridge, Mass. 02139-1901; 617-577-1017; fax, 617-577-8829; or* **circle 110.**

Playing the market

If you have a few dollars to invest and prefer to base your investment decisions on something other than marketing hype and salesmen's pitches, you may be drawn to a computer program written by a fellow engineer. David Chamness, a mechanical engineer at a major electronics company, wrote the stock market forecasting program for his own use, but found his colleagues interested enough in having their own copies to pay for them. So he cleaned it up, wrote a manual, formed a company, and is offering it for sale.

The program forecasts values three, six, and 12 months ahead for the Standard & Poor's (S&P) 500, Treasury Bond rates, Treasury Bill rates, and the Consumer Price Index (CPI). It bases its predictions on mathematical models derived by applying linear regression analysis to the 25 years of market history from 1963 through 1989.

To use the program, you enter eight parameters, specifically, the S&P 500 close, prime rate, Treasury Bond rate and Treasury Bill rate, CPI, unemployment rate, S&P 500 dividend yield, and S&P 500 price/ earnings ratio.

In addition to the forecasting routine, the program has an asset allocation routine, which tells you how much of each asset to hold with conservative and aggressive investment strategies.

The menu-driven program runs on IBM PCs and compatibles. It requires DOS 2.0 or higher plus 256K bytes of RAM. A hard disk is optional.

The program is priced at $39.99. *Contact: DC Econometrics, 2920 Mount Royal Court, Fort Collins, Colo. 80526; or* **circle 111.**

POWER AND ENERGY

A high-'tec ac power line monitor

With electronic equipment making up an ever increasing fraction of the load on electric utilities, the issue of power quality is growing in importance. More and more, users of computers and precision measuring equipment are finding that erroneous results and even equipment damage can sometimes be due to power line spikes or other kinds of contamination.

Even Dr. Watson can detect power line problems like spikes, sags, and surges with the help of the Sherlock power analyzer.

Clearly, the first step in dealing with contaminated power is determining whether it indeed exists at a particular location. An unusually cost-effective tool for making that determination is the Sherlock, a portable power line analyzer with a price tag of just $995.95. (Of course, analyzers already exist that can do the job, but they are more sophisticated, higher-priced instruments.)

Sherlock plugs into a power socket and monitors it continuously, looking for 15 types of events, which it captures and stores in nonvolatile memory for analysis. Among the events are spikes on the hot line, sags, surges, high-frequency noise, phase changes, frequency deviations, and ac line dropouts.

Sherlock keeps detailed information on the first hundred events in each category, for a total of 1500 events. Details include date and time of occurrence, event magnitude, and location of the event on the power sine wave. After 100 events have been acquired in a given category, it stores cumulative totals—up to 256 000 events per category, for a total of 3 840 000.

Stored data may be retained for up to five years in battery-backed RAM, printed out, and/or downloaded into a PC for analysis. A companion power analysis software package selling for $199.95 processes the data into colorful graphic displays like pie and bar charts. *Contact: DSK Power Products Inc., 538 S. 1400 W. (Commerce Rd.), Orem, Utah 84058; 801-224-4828; fax, 801-224-5872; or* **circle 112.**

GENERAL INTEREST

Budget LCD color projectors

The big project is finished and it's time to begin the presentations—to top management, potential customers, and the press. It would help if you had a high-quality liquid-crystal display (LCD) color projection panel to interface your computer with a standard overhead projector. But you've always shied away from them because of their cost—typically $6000 to $9000.

ColorWorks may change that picture. A lightweight (2.7 kg) panel, it can project 24 389 colors with a contrast ratio of 20:1, and it costs only $3995. If your presentation does not need video or sophisticated animation, it may be just what you need.

Most entry-level systems attain color by stacking three passive-array LCD panels (one for each of the primary colors) on top of each other. But ColorWorks uses color-stripe filter technology to incorporate all three hues on one panel. In addition to reducing size, weight, and cost, that approach boosts color saturation and contrast ratio.

Because it uses a passive-matrix panel, ColorWorks does not have the speedy response time (30 to 50 ms) of top-end active-matrix panels. It is therefore not suitable for displaying TV video with lots of motion. On the other hand, thanks to continuing improvements in LCD technology, it is fast enough (around 100 ms) to handle video without a lot of motion and camera pans.

The product comes in two models, both of which include wireless remote control and all the cabling needed for VGA and Macintosh II presentations. The A502C has a 9-inch diagonal panel whereas the A522C, which is priced at $4995, has a 11-inch panel. The A522C also comes with presentation utility software and additional cabling. *Contact: Proxima Corp., 6610 Nancy Ridge Dr., San Diego, Calif. 92121-3297; 619-457-5500, ext. 246; fax, 619-457-9647. In Europe, Proxima International, Horsterweg 24, 6191 AD Beek, Maastricht, the Netherlands; (31+43) 65 02 48; or* **circle 113.**

COORDINATOR: Michael Riezenman
CONSULTANT: Paul A.T. Wolfgang, Boeing Defense & Space Group

Software reviews

Specifying a human-machine interface

Avi Zahavi

Rapid 1.0 *Software for the interactive, point-and-click specification and execution of user interfaces for embedded, event-driven systems. The version reviewed runs under Microsoft Windows 3.X. US $8000.*

Rapid is a truly comprehensive software package for the system designer who would like to create and try out human-machine interfaces interactively and enhance the functionality of the result incrementally. It is best suited for designs that must deal with numerous inputs occurring at unpredictable intervals. Using Rapid's set of object-oriented graphical tools, system engineers or designers can specify real-time embedded systems with precision and simulate their dynamic properties with rigor.

The software is easy to install and well documented. The manual takes the designer through the process of building a small application, encouraging him or her to move ahead and explore the product's other capabilities with a second, very detailed, training guide. This guide gives hands-on experience of Rapid's most important features and hence a comprehensive understanding of how to build an application. For a complete technical reference, the Rapid language guide explains the underlying formalism and further supplements the manual with application examples.

Rapid's integrated environment provides four main modules—the object editor, logic editor, logic chart, and prototyper—all supported with an on-line, context-sensitive help. In addition, a report generator describes the objects and application logic, and a logic tester examines the consistency and completeness of the logic definition.

The object editor is used to specify both graphic and non-graphic objects. Graphic objects have a graphical representation that can be customized to appear as the elements in the target system. Rapid supplies a rich set of object classes, including indicator lamps, push-buttons, text display, and switches, and each class in turn represents a variety of objects. For example, a switch object may be selected from a set of toggle, rocker, rotary, slider, and stepper switches. Once an object is selected, additional properties such as location, size, name, and color can be specified. The non-graphic objects fall into three categories: time-related (timer, stopwatch, real-time date, and clock); data-related (number objects or string objects); and audio-related.

Next the designer, having defined the objects for the application, employs the logic editor to specify the application's logic structure and behavior. Using dialog boxes, pull-down menus, and point-and-click techniques, the designer builds the application's hierarchical mode tree and defines the transitions between the modes. The modes represent the various states in which the system can be. Then, in a highly visual and structured manner, the designer specifies the transitions among the modes, the triggers, the actions, and the activities that determine the application's dynamic behavior.

At that point, the designer is ready to run the application using the prototyper module. Controls such as switches, potentiometers, and push buttons are operated by clicking the mouse as soon as it has steered the cursor onto the object's graphical representation. The output (such as text displays, dials, and lamps) changes according to the application logic in response to the user's input or other time-related triggers.

The logic chart module complements the logic editor by automatically generating and displaying a graphic, bird's-eye view of the logic definition in a state diagram format. The designer is also able to specify the output's level of detail, or granularity, and abstraction by zooming in and out of the logic charts.

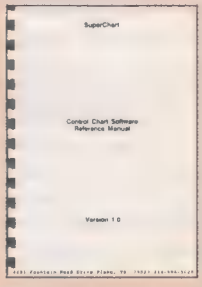
Performance was smooth on my 486/33-MHz PC with its 8M bytes of RAM. Nevertheless, Rapid was noticeably slow at starting up, as well as at reading and saving applications to the hard disk. On the other hand, the user interface is exceptionally intuitive and well designed. As I grew more comfortable with Rapid, I tried exploring various short cuts, which, to my surprise, had already been thought of and implemented by Rapid's designers. It is worth mentioning that the company also offers other add-on Rapid modules, not tested by this reviewer. One such module provides the ability to drive an external product like an industrial controller via the RS-232 port or Windows' dynamic data exchange (DDE) mechanism, which converts the prototype into an interface to the real application.

In summary, I was pleasantly surprised to see a very professional PC software product that normally I would associate with the computational power of a workstation environment. If you are in the market for such a product, I would strongly recommend this one. It is a cost-effective and well-implemented package. *Contact: Emultek Ltd., Yuvalim 20142 D.N., Misgav, Israel, (972+4) 800 028; fax, (972+4) 800 460; or* **circle 100.**

Avi Zahavi is a senior consultant to AT&T Co. and Bell Laboratories in a variety of software development and engineering projects.

Keeping control

John R. Hines



SuperChart 1.0, SuperChart/SPC Charts. *Software for statistical process control. The version reviewed requires at least an IBM PC XT or compatible with EGA display, DOS 3.0 or higher. US $145 for single copies.*

This statistical process control (SPC) program creates and maintains high-resolution SPC charts, both on-line and hard copy, yet is low cost and easy to use. It uses the methodology and formats described in Donald J. Wheeler and David S. Chambers's *Understanding Statistical Process Control* (Statistical Process Controls, 1986), a widely used text, so its charts are statistically correct and generic.

SuperChart generates nine types of charts, five for measurement data and four for count data for various kinds of manufacturing data. The charts are created, edited, and printed by means of function keys; pressing the F1 key summons on-line help describing what each key does.

Of special interest are the program's on-line action plans, its out-of-control log, and its network capability. The action plans are text files that may be created and edited with a text editor and viewed from SuperChart; numbered items on such a plan may indicate corrective actions taken when a chart shows a process is out of control, and may also flag process changes that could cause problems in the chart. The out-of-control log, also a text file, lists charts that indicate processes that have run amok during the past 24 hours; it allows engineers or supervisors to manage by exception, identifying out-of-control operations immediately. Lastly, network capability makes everything—action plans, the out-of-control log file, and SPC charts—for every operation accessible from every networked computer. Without leaving his or her desk, an engineer can review processes

READER GUIDE TO PRODUCTS AND SERVICES

1991 IEEE
U.S. Membership Salary
and Fringe Benefit Survey

The only source of current information on the salaries and fringe benefits of electrical engineers in the United States is now more comprehensive and informative than ever before. Explores more than 50 variables affecting salaries and benefits. Shows salary variation by Metropolitan Statistical Areas, traces salaries vs. Consumer Price Index from 1972, and shows frequency distribution of all statistics. Contains more than 75 exhibits. Essential data for engineers, corporate and engineering managers, and personnel and salary administrators.

Product No.	Member	List
UH0185-9	$74.95	$99.95

To order, call 1-800-678-IEEE or 908-981-0060 outside the United States.

The Standards Tool
for Today's Power Engineer

IEEE STANDARDS COLLECTIONS

For many engineers, purchasing groups of similar standards individually may not be practical or economical. Typically, engineers require groups of standards that deal with specific technologies. When packaged together, these standards collections prove invaluable to today's engineers, making it easier for them to perform their jobs effectively.

Now available:
IEEE C57 Standards Collection, Winter 1992 Edition
Distribution, Power, and Regulating Transformers

Updated to include 63 of the most current IEEE and ANSI standards on power distribution and regulating transformers, the IEEE C57 Collection is a must for today's power engineers worldwide.

ISBN 1-55937-182-X Product Number: SH14902
IEEE Member Price: $94.50 List Price: $135.00

Order today and enjoy the convenience and savings provided by IEEE Standards collections.

Call toll-free 1-800-678-IEEE in the United States and Canada. Outside the United States and Canada, call 908-981-1393.

For more information on IEEE Standards Collections, CIRCLE #81 on the Reader Service Card.

NEW
IEE BOOKS

Algorithmic and Knowledge-Based CAD for VLSI $72.00
G. E. Taylor and G. Russell (Eds.)
This sampling of the present state of the art in computer-aided design (CAD) for very large-scale integration (VLSI) covers newly developed algorithms and applications of techniques from the artificial intelligence (AI) community.
288 pp., 229 by 148 mm, casebound
ISBN 0-86341-267-X—1992 Circuits & Systems Series #4

Applied Artificial Intelligence $65.00
K. Warwick (Ed.)
This book provides an introduction to the selection and application of artificial intelligence tools.
240 pp., 229 by 148 mm, casebound
ISBN 0-86341-245-9—1991 Computing Series #19

Neural Networks for Control and Systems $72.00
K. Warwick, G. Irwin, and K. Hunt (Eds.)
This introduction to the present state of neural network research and development is also an overview of the field, with particular reference to systems and control application studies.
260 pp., 229 by 148 mm, casebound
ISBN 0-86341-279-3—1992 Control Series #46

Artificial Neural Networks $104.00
Second International Conference
This book highlights conference proceedings, held November 18–20, 1991, at Bournemouth International Centre, Bournemouth, United Kingdom.
383 pp., 72 papers, 297 by 210 mm, softcover
ISBN 0-85296-653-11—1991 IEE Conference #349

ALL MAJOR CREDIT CARDS ACCEPTED
Call or write IEEE Service Center, PPL Department, 445 Hoes Lane, Piscataway, N.J. 08855-1331; 908-562-5553; fax, 908-981-0027.

For our latest publications catalog, CIRCLE #82 on the Reader Service Card.

IEEE
STANDARD COMPUTER DICTIONARY

The Complete Resource for
Today's Computer Terminology

With the field of computer engineering expanding, new computer terms are constantly being defined just as new meanings are being adopted for existing terms. Computer professionals have been in dire need of a reliable source for standardized definitions that are current and accurately reflect the terms as-

(Continued overleaf)

READER SERVICE (CIRCLE NUMBERS)

1 PRODUCT INFORMATION

1	10	19	28	37	46	55	64	73	82	91	100	109	118	127	136	145	154	163	172
2	11	20	29	38	47	56	65	74	83	92	101	110	119	128	137	146	155	164	173
3	12	21	30	39	48	57	66	75	84	93	102	111	120	129	138	147	156	165	174
4	13	22	31	40	49	58	67	76	85	94	103	112	121	130	139	148	157	166	175
5	14	23	32	41	50	59	68	77	86	95	104	113	122	131	140	149	158	167	176
6	15	24	33	42	51	60	69	78	87	96	105	114	123	132	141	150	159	168	177
7	16	25	34	43	52	61	70	79	88	97	106	115	124	133	142	151	160	169	178
8	17	26	35	44	53	62	71	80	89	98	107	116	125	134	143	152	161	170	179
9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144	153	162	171	180

MEMBERSHIP INFORMATION

300 Regular 301 Student

Print or Type only
Name _____ Title _____

Company _____

Address _____

City _____ State _____ Zip _____

Country _____ Business Phone _____

If this represents a change in address, please fill out form on p. 9

3 ADDITIONAL COMMENTS

_____

_____

I would like: _____

DELIVERY: I received this issue _____ (date).

For faster information, fax this card to 413-637-4343

Void after November 1, 1992 *Void overseas December 1, 1992*

8

READER FEEDBACK (CIRCLE NUMBERS)

2 EDITORIAL MATTER

Article/Item	Comment: Too Simple	Too Technical	Too detailed
Information security			
Threats and countermeasures	01	02	03
Cryptography and the NSA	04	05	06
Computer viruses: a tutorial	07	08	09
Roundtable	10	11	12
Reliability handbook	13	14	15
Superconducting consortium	16	17	18
Software reliability	19	20	21
Profile: Hackwood	22	23	24
Smith chart	25	26	27
Newslog	28	29	30
EEs' tools & toys	31	32	33
Technically speaking	34	35	36
Software reviews	37	38	39
Faults and failures	40	41	42

Did you find this material stimulating or thought-provoking?

Item	Yes	No
Spectral lines	43	44
Forum	45	46
Books	47	48

sociated with technologies of today's computer industry.

Now, computer professionals can have access to all these definitions in one convenient volume—*IEEE Standard Computer Dictionary, Compilation of IEEE Standard Computer Glossaries*. This is a complete collection of terms from the six existing IEEE Standard Glossaries, and accurately documents the most current computer industry vocabulary.

IEEE Std 610-1990, *IEEE Standard Computer Dictionary, Compilation of IEEE Standard Computer Glossaries*
ISBN 1-55937-079-3
Product Number: SH13857
IEEE Member Price: $45.50
List Price: $65.00

To order, call 800-678-IEEE. Outside the United States, call 908-981-1392.

For more information, CIRCLE #83 on the Reader Service Card.

NEW BOOKS FROM THE IEEE PRESS

DIGITAL MOS INTEGRATED CIRCUITS II
With Applications to Processors and Memory Design
Edited by Mohamed I. Elmasry, University of Waterloo, Ontario, Canada

Representing today's key research work in digital MOS integrated circuits, this book offers the most comprehensive, up-to-date information on a field that has witnessed phenomenal advances over the past 10 years. Of great value to MOS digital circuit and system designers as well as researchers, *Digital MOS Integrated Circuits II* covers the most recent developments in digital MOS ICs and their applications in memory, signal and data processing, and application-specific ICs.

December 1991 ISBN 0-87942-275-0
Order #PC02691-PNE Approx. 488 pp.
IEEE Member Price: $55.00 List Price: $69.95

UNDERSTANDING LASERS*
An Entry-Level Guide
by Jeff Hecht Sr., Contributing Editor, *Laser and Optronics Magazine*

This introductory guide explains how lasers work and how they are used in the real world of medicine, telephones, compact discs, and supermarket checkout lanes. Written for students, hobbyists, and the just plain curious, this authoritative text is clear, succinct, and amply illustrated—an ideal tool and a valuable reference for technical and nontechnical readers alike.

November 1991 ISBN 0-87942-298-X
Order #PP02931-PNE 448 pp., softcover
IEEE Member Price: $20.00 List Price: $24.95

*This is the IEEE edition of a book previously published by Howard W. Sams and Company under the title *Understanding Lasers.*

To order, call 1-800-678-IEEE. For more information, CIRCLE #84 on the Reader Service Card.

1993 NATIONAL ELECTRICAL SAFETY CODE

Adopted by 48 states and the majority of Public Service Commissions nationwide, the National Electrical Safety Code (NESC) is the single most important document today for safeguarding persons against electrical hazards during installation, operation, and maintenance of electric supply and communication lines.

On August 3, 1992, the IEEE will publish the 1993 edition of the NESC. Also this August, IEEE Standards Press will be publishing the NESC Handbook—today's essential NESC "user guide." This latest edition of the handbook covers NESC requirements up to 1993, detailing various work rules and providing a historical perspective of the code.

Make sure you have the code and handbook as soon as they're published—so you can put the latest code provisions to work for you. Place your prepublication order today!

Look for NESC and NESC Handbook Set this August.

Together the NESC and NESC handbook provide all the critical safety and technical information you need, plus the practical guidance to put it to use.

When you purchase both publications together in this set, you save over 20 percent off regular list prices!

C2-1993 National Electrical Safety Code
ISBN 1-55937-210-9
Product Number: SH15172
IEEE Member Price: $26.95 List Price: $39.50

NESC Handbook ISBN 1-55937-211-7
Product Number: SP00042
IEEE Member Price: $45.50 List Price: $65.00

1993 NESC and NESC Handbook Set
ISBN 1-55937-214-1
Product Number: SH15339
IEEE Member Price: $70.00 List Price: $80.00

To order by phone, call 800-678-IEEE, 8 a.m.–4 p.m. (EST). Outside the United States and Canada, call 908-981-1393.

For more information, CIRCLE #85 on the Reader Service Card.

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

BUSINESS REPLY MAIL
FIRST CLASS MAIL PERMIT NO. 885, PITTSFIELD, MA
POSTAGE WILL BE PAID BY ADDRESSEE

IEEE SPECTRUM
READER SERVICE MANAGEMENT DEPT.
PO BOX 5149
PITTSFIELD, MA 01203-9740

Software reviews

running in another part of the building or in ▪ building down the street or in another city.

The on-line charts produced by SuperChart are colorful and readable. An observer 1.5 meters or more from a 13-inch VGA monitor can easily see trends, so the program is ideal for use in ▪ manufacturing environment. Hard copy charts are readable but not as attractive as the screen display. Being simply black-and-white reproductions of the on-line charts, they ignore the higher resolution offered by laser printers or dot matrix printers.

SuperChart has three weaknesses, though: low speed, ▪ dated interface, and deficient documentation. As ▪ graphical program, SuperChart is slow. When Honeywell Inc.'s Micro Switch Division, Richardson, Texas, started using SuperChart on XT-compatible workstations in its semiconductor manufacturing area, operators reported the response time too slow for analysis or trouble shooting. Upgrading the XTs with 286 or 386SX mother boards eliminated these complaints. Still, if the only purpose is to display data and not to do analysis on XTs, SuperChart works fine.

SuperChart's function key interface is old-fashioned. While usable, it does not correspond to the keystrokes that come automatically to DOS 5 or Windows users of the WiMP (windows, mouse, and pull-down menus) CUA (common user access) interface.

Finally, the documentation is weak. The manual has neither index nor detailed information on specific features. Fortunately, few users will ever need to look at it, the on-line help is so good. *Contact: SuperChart/SPC Charts, 2401 Fountain Head Dr., Plano, Texas 75023; 214-596-5020; or* **circle 101.**

John R. Hines (M) is a silicon engineer at Honeywell Inc.'s Micro Switch Division, Richardson, Texas.

COORDINATOR: Gadi Kaplan

Recent software

Worst-Case Analyzer (WCA) 2.0. A math-based software tool for design validation. For IBM PCs and compatibles with 512K memory and ▪ hard drive. Including *The DACI Worst-Case Analysis Handbook*, US $595. *Contact: Design Analysis Consultants Inc. (DACI), 10014 N. Dale Mabry, Suite 101, Tampa, Fla. 33618-4426; 813-265-8331; or* **circle 102.**

DigiMatic v2.0. An upgrade of earlier software that converts graphic information into numerical data and adds an automatic screen scanning support. Compatible with all Macintosh computers. US $249. *Contact: Famous Engineer Brand Software, 4855 Finlay St., Richmond, Va. 23231; 804-222-2215; fax, 804-226-1934; or* **circle 103.**

PlotIT 2.0. A new version of an earlier package for transforming data into charts and graphs on DOS-based personal computers (and ▪ variety of minis and mainframes). New features include:

- Direct reading of database files, spreadsheet and ASCII files.
- ▪ A selection of high-quality outline fonts, as well as easy access to third-party fonts.
- Enhanced autoscaling capability.
- ▪ Simultaneous composition and editing of multiple graphs, and more. US $495 (DOS). Prices for minis and mainframes, available on request. *Contact: Scientific Programming Enterprises, Box 669, Haslett, Mich. 48840; 517-339-9859; fax, 517-339-4376; or* **circle 104.**

InterTools. Software development tools for IBM PC and Sun workstations for the NEC 77240 digital signal processor (US $2500 and up). *Contact: Intermetrics Microsystems Software Inc., Cambridge, Mass. 01238; 800-356-3594; or 617-661-0072, or* **circle 105.**

Faults & failures

The 747 door on the ocean floor

New evidence dredged from the deep faults an electrical switch and wiring for causing a serious accident originally attributed to poor mechanical maintenance. The accident occurred on Feb. 24, 1989, shortly after United Airlines flight 811 took off from Honolulu for Auckland, New Zealand. As the Boeing 747, model 122, reached 6800 meters altitude above the Pacific Ocean, a cargo door suddenly flew open and broke away from the fuselage, taking with it the skin and the parts of the structure just above it. In the explosive decompression that followed, nine passengers were ejected through the hole torn in the cabin and lost at sea.

The cockpit crew shut down two of the plane's four engines, which had ingested debris from the cargo door and fuselage, and immediately turned back to Honolulu airport, landing the crippled plane in early-morning darkness about 40 minutes after they had departed.

An investigation ensued, and about 14 months later the U.S. National Transportation Safety Board (NTSB) issued an accident report. In it, the cause of the accident was said to be a damaged cargo-door locking mechanism, which appeared to be locked when it was not.

The NTSB based its conclusion largely on the history of the plane's cargo door, which had had repeated problems with closure.

The locking mechanism consists of eight latch pins, on the cargo door sill, that engage eight latch cams on the door when it closes. A ground crew member, outside the aircraft, then pushes a button to electrically rotate the latch cams 80° clockwise into their fully latched position [see figure] and pushes a master handle to rotate the eight lock sectors over the latch cams and latch pins, thereby securing the door.

The board hypothesized that the ground crew must have omitted the step of pushing the button to turn the latch cams, and then, when they pushed the master handle, the lock sectors must have been so bent and battered that they easily passed over the unlatched cams. When the door closed, a lamp on the flight engineer's cockpit panel would have gone out, indicating falsely that the cargo door had been secured.

The NTSB, United Airlines, and the Boeing Airplane Co. nevertheless still wanted to recover the door and knew approximately where it was on the ocean floor. In July 1990, the U.S. Navy mounted an underwater search.

A towed sonar scanner located a debris field on the ocean floor, 4300 meters below the surface, on its first pass over the suspect area. The Navy's *Sea Cliff* deep-sea vehicle then made dives to the site.

On the sixth dive, the crew found the lower part of the cargo door, brought it to the surface, and transferred it to the accompanying Navy ship, *Laney Chouest*. On the eighth and last dive, they recovered the upper part of the door.

Frank Hilldrup, a structures specialist at NTSB, examined the door parts as soon as they were set on the *Laney Chouest*'s deck. Contrary to expectations, he found that the lock sectors were not severely bent and gouged. In fact, their position showed that they must have fully locked the latch cams when the door had been shut. What was remarkable was that the latch cams were in a partly open position and had apparently counterrotated after door closure, damaging the lock sectors as they did so [see figure].

Testifying later at an NTSB hearing on the new evidence, Hilldrup said, "We know for a fact that the door was closed properly. . . [and] that the latch cam was rotated open after things were secured properly."

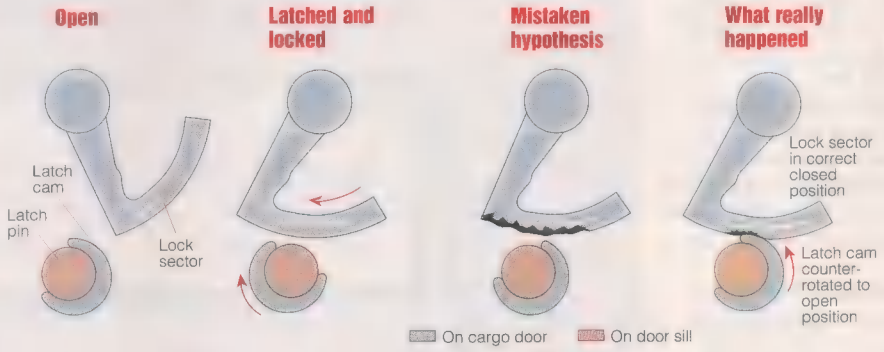
How that counterrotation occurred became clearer as the investigators continued their examination of the recovered door and sifted through maintenance records for Boeing 747-122s. They found that—with one exception—the electrical components on the door were properly installed and functional, although they had been damaged from being submerged at great depth in the sea. The exception was the master lock switch, a contact switch designed to cut off power to the latch cam motors after they have rotated to the latched position. That switch was found to be stuck in the ON position on Flight 811's cargo door—a position that would allow the motors to counterrotate if a spurious signal activated the door's control logic.

Tracing the door's wiring schematic, the investigators found that a short circuit at any of several points could create such a signal. Further, examining what remained of the door's wires, they found spots with exposed conductor. The NTSB investigators reasoned that the wires, part of a bungee-held bundle that rises out of the way when the door is opened, were abraded by repeated door openings and closings and by passing cargo containers.

Once the cause had been pinpointed with reasonable certainty, the preventive measures were obvious, and have since been implemented by the airplane manufacturer. The lock sector has been strengthened so that it fully resists any tendency of the latch cam to backdrive (the sector is now made of steel instead of aluminum). As further insurance against counterrotation damage, torque limiters have been installed on the latch cam motors. And sensors and logic circuitry now monitor the latch cams after the master latch has been activated.

Frequent inspection of the door's wire bundle is now required, and it has been enclosed in an improved sheath to protect it from abrasion. Finally, the cargo-door-open indicator circuit has been redesigned so that it determines whether the door has truly been latched and locked.

The amended report is now available as document PB92-910402 from the National Technical Information Service, 5285 Port Royal Rd., Springfield, Va. 22161; 703-487-4650; fax, 703-321-8547.



Lock sector can swing into locked position only when latch cam has rotated clockwise unless the sector is bent and gouged. Actually, the cam counterrotated under the locked sector.

COORDINATOR: George F. Watson
CONSULTANTS: John Devaney, High-Rel Laboratories Inc.; Robert Thomas, Oneida Research Services

CLASSIFIED EMPLOYMENT OPPORTUNITIES

The following listings of interest to IEEE members have been placed by educational, government, and industrial organizations as well as by individuals seeking positions. To respond, apply in writing to the address given or to the box number listed in care of *Spectrum* Magazine, Classified Employment Opportunities Department, 345 E. 47th St., New York, N.Y. 10017.

ADVERTISING RATES

Positions open—$36.00 per line, not agency-commissionable

Positions wanted—$36.00 per line, a 50% discount for IEEE members who supply their membership numbers with advertising copy

All classified advertising copy must be received by the 25th of month, two months preceding date of issue. No telephone orders accepted. For further information contact Francesca Silvestri, 212-705-7578.

IEEE encourages employers to offer salaries that are competitive, but occasionally a salary may be offered that is significantly below currently acceptable levels. In such cases the reader may wish to inquire of the employer whether extenuating circumstances apply.

Academic Positions Open

Position Open: The Dept. of BME of the University of Miami seeks applications and nominations for a new tenure track faculty position at the Asst. Prof. rank, for the Fall '92 semester, with the following minimum qualifications: PhD in Engineering or in a closely allied field; research experience in BME; demonstrable interest in the development and teaching of undergraduate level lecture and lab courses in BME. The 9-month appointment may be extended for summers. Salary and fringe benefits are competitive. The University of Miami is an equal opportunity employer. Please contact: Dr. Ozcan Ozdamar, Dept. of BME, College of Engineering, University of Miami, POB 248294, Coral Gables, FL 33124.

Australian National University—Research School of Physical Sciences and Engineering—Optical Sciences Centre-Fellow/Senior Fellow—(Academic Level C/Academic Level D). Applications are invited for appointment to a continuing (on probation) research-only position at academic level C or D in the Optical Sciences Centre (Head: Professor A W Snyder, FRS), Research School of Physical Sciences and Engineering. Here is a unique opportunity for an exceptionally creative theoretical research scientist to work with a dynamic interdisciplinary research team at the forefront of new ideas and applications in guided wave optics. The Centre, within the prestigious Institute of Advanced Studies, allows one to concentrate exclusively on research in an environment marvelously conducive to creating original ideas. Activities in the Centre span the nonlinear phenomena of light-guiding-light, spatial solitons, optical switching, active devices and chaos, and also embrace the design of miniaturized planar optical devices and circuitry for the revolutionary photonic chip. The Centre is a pivotal player in major collaborative projects initiated by the exciting new $100 million Australian Photonics Cooperative Research Centre, linking academic excellence with the major telecommunications industries. The successful candidate will be expected to provide dynamic leadership and accept responsibility within these areas. Enquiries may be made to Professor Snyder, telephone (international) 61 6 249 2626. Closing date: 1 August 1992. Ref: PSE 20.5.2. Salary: Fellow—$A50,225—$A57,913 pa.; Senior Fellow—$A57,913—$A66,625 pa. (from 23 July 1992). Appointment: Fellow/Senior Fellow continuing (on probation). Applications, clearly quoting reference number, should be submitted in duplicate to the Secretary, The Australian National University, GPO Box 4, Canberra ACT 2601, Australia including curriculum vitae, list of publications and names of at least three referees. Further information including Selection Criteria is available from the Secretary. The University is an Equal Opportunity Employer.

The Australian National University—Research School of Physical Sciences and Engineering—Computer Sciences Laboratory - Fellow/Senior Fellow—(Academic Level C/Academic Level D). Applications are invited for appointment to a continuing (on probation) research-only position at academic level C or D in the Computer Sciences Laboratory (Head: Professor R P Brent, FAA), Research School of Physical Sciences and Engineering. The Computer Sciences Laboratory is a Department within the Engineering Division of the Research School of Physical Sciences and Engineering, and has close ties to the Department of Computer Science (Faculty of Science) and the Centre for Information Science Research. Current research includes design and analysis of parallel algorithms; software development, software tools and scientific applications on parallel (MIMD and SIMD) computers; aspects of human-machine systems, including speech recognition, speaker characterization, image analysis and processing. Facilities include access to several parallel machines, including a 128-cell Fujitsu AP1000, a 16384-processor Connection Machine (CM2), a Fujitsu VP2200/10 vector processor, and a 16-node Transputer system. Applicants should have a strong research record in one of the areas mentioned above, or in a related area of the Computer Sciences. Duties include independent research, supervision of postgraduate students, and involvement in appropriate professional activities. Enquiries may be made to Professor Brent, telephone (international) 61 6 249 3329, email rpb@cslab.anu.edu.au. Closing Date: 31 August 1992. Ref: PSE 20.5.3. Salary: Fellow—$A50,225—$A57,913 pa.; Senior Fellow—$A57,913—$A66,625 pa. (from 23 July 1992). Appointment: Fellow/Senior Fellow Continuing (on probation). Applications, clearly quoting reference number, should be submitted in duplicate to the Secretary, The Australian National University, GPO Box 4, Canberra ACT 2601, Australia, including curriculum vitae, list of publications and names of at least three referees. Further information including Selection Criteria is available from the Secretary. The University is an Equal Opportunity Employer.

Ameritech Chair in Information Technology in Electrical Engineering and Computer Science. The Department of Electrical Engineering and Computer Science of the Robert R. McCormick School of Engineering and Applied Science at Northwestern University is soliciting nominations and applications for an endowed chair by the Ameritech Foundation in the area of Information Technology. The Chair will be involved in teaching and research in the area of information technology which includes information networks, telecommunications, information management, and other related high-tech areas. The Chair is expected to play a leading role in the College interdisciplinary Center for Information and Telecommunication Technology, as well as provide leadership in graduate educational programs in the information technology and telecommunications areas. The information technology area is very active at Northwestern University with support from the information industry, including Ameritech. The endowment for the Chair as well as the existing research and educational programs will provide an excellent opportunity for success. Candidates for the Ameritech Chair must be teachers and researchers of great distinction with a record of significant achievements and international reputation in the field. We seek candidates with either industrial and/or academic experience in one or more of the topics covered under the area of information technology. The deadline for nominations and application is October 1, 1992, but the search will continue until a suitable candidate is found. Please send nominations or applications to: A.H. Haddad, Chairman, Electrical Engineering and Computer Science, Northwestern University, 2145 Sheridan Road, Evanston, IL 60208-3118, Phone: (708) 491-3641. Northwestern University is an equal opportunity, affirmative action employer. Applications from women and minorities are encouraged. Employment verification required upon hire.

University of Wisconsin-Madison—Faculty Position. The Department of Electrical and Computer Engineering invites applications for a possible tenure or tenure-track position. A Ph.D. degree is required, and the successful candidate is expected to establish a strong research program and participate in a high quality instructional program. Applicants in all areas of computer engineering are invited to apply. Rank and salary will be commensurate with qualifications and experience. Send resume and names of three references to Bahaa E.A. Saleh, Chairman, Department of Electrical and Computer Engineering, University of Wisconsin-Madison, 1415 Johnson Drive, Madison, WI 53706, an equal opportunity/affirmative action employer. Names, titles and/or occupations, and addresses of applicants and nominees cannot be kept confidential.

Tenure Track Faculty Position—University of Notre Dame. The Department of Electrical Engineering invites applications in the area of Electronic Materials. Special attention will be given to individuals specializing in materials growth or processing. Applicants should have a Ph.D. in Electrical Engineering, Materials Science and Engineering, or a related field. The Department offers B.S., M.S., and Ph.D. programs in Electrical Engineering and M.S. and Ph.D. programs in Materials Science and Engineering. Active research areas include semiconductor materials and devices, materials characterization, device simulation, and high temperature superconductors. Applicants should have interest in teaching at the undergraduate and graduate levels, advising students, and conducting research. Rank and salary are negotiable. Interested persons should submit a complete resume and names of three references to: Dr. Daniel J. Costello, Chair, Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556. The University of Notre Dame is an Affirmative Action/Equal Opportunity Employer.

Ph.D. Student: The ECE Department of the University of South Carolina is seeking a bright Ph.D. student to pursue a thesis in "High Field Effects in Bandgap Materials under Pulsed and RF Fields." The materials include Si, GaAs, ceramics, and diamond. Experience in electrical and optical diagnostics preferred. US citizen. Send resume to Prof. T.S. Sudarshan, College of Engineering, USC, Columbia, SC 29208.

Stanford University—Department of Electrical Engineering - Professor (Research). Stanford University, Dept. of Elect. Eng., Information Systems Laboratory seeks applications for a Professor (Research) position in signal processing. The position will involve creating a strong interdisciplinary group to span algorithms development, computational methods, digital signal processing architectures, and practical implementation of the applications of array signal processing. The thrust of this new Professor (Research) position is to accelerate the transition to practice of recent theoretical developments. The candidate should have a Ph.D. and have a strong background in systems development with experience in array signal processing systems coupled with some experience in digital signal processing architectures. An equally strong record of research contributions to the theoretical underpinnings of the above areas is essential. Prior experience in both industrial R&D and academic research settings is desirable. The position needs a candidate with an exceptionally strong ability to work in a multidisciplinary setting applying both the theory and the prac-

tice of signal processing and computing to applications in communications/manufacturing systems. This is strictly a non- tenure-track position and has no teaching duties, although occasional teaching opportunities may be available. The candidate will have to supervise the research of Ph.D. students and is expected to work closely with industry. Financial resources for Professor (Research) (including salary, student support and overheads) will have to be earned entirely through research contracts from industry/government as per existing university regulations. Stanford University is an Equal Opportunity Employer and encourages applications from women and minority candidates. The deadline for receipt of applications is August 15, 1992. Please submit a detailed resume, a publication list and the names of five references to Prof. Umran S. Inan, Dept. of Electrical Engineering, Durand 321, Stanford University, Stanford, CA 94305-4055.

New Zealand University of Canterbury—Post-Doctoral Fellowship (Optical Communications). Applications are sought for the position of Post-Doctoral Fellow in the Department of Electrical and Electronic Engineering. The position is for ■ duration of two years and applicants should be able to commence work by 2 March 1993. Applicants should have recently completed, or be in the process of completing, ■ doctorate in Physics or Electrical Engineering and have abilities in the general area of optical communications. Some background in modulation and coding would also be helpful. Preference will be given to someone who has some experimental experience. The successful applicant will work with two researchers and their team of graduate students in research related to the changes in polarized light in fibre transmission systems, fibre amplifiers and soliton systems. The Department is well-equipped with SUN, VAX, workstations and IBM-family personal computers as well as ■ modestly equipped optical laboratory. The emolument for a Fellowship shall be at a rate not exceeding the lowest step of the Lecturer salary scale (NZ$37,440 per annum). The University is not able to pay for additional travel expenses for the Fellow to take up the appointment, but help is provided in finding convenient accommodation. The city of Christchurch is well served by recreational activities including world-class skiing, sea and land waterways and ready access to excellent walking tracks. Before submitting a formal written application, candidates are requested to obtain Conditions of Appointment from the undersigned. Applications, quoting Reference Code C92/01, close on 30 September 1992 and should be addressed to: A.W. Hayward, Registrar, University of Canterbury, Private Bag 4800, Christchurch, New Zealand. The University has a policy of equality of opportunity in employment.

Yale University—Electrical Engineering. The Department of Electrical Engineering invites applications for a faculty position at the Assistant or Term Associate Professorial level in VLSI system design, computer architecture, parallel processors, and other areas of computer engineering. Applicants should have ■ Ph.D. in Electrical Engineering, Computer Science, or closely related field, and should exhibit outstanding research accomplishments and a commitment to teaching. Close collaboration with the existing computer engineering group in the Department and interaction with the Department of Computer Science are desired. Preferred candidates should also have a strong interest in other programs in the Department, including microelectronics, systems science, and signal processing, and would be expected to contribute to joint research activities. Applications are accepted until October 30, 1992. Please send resume, including names, addresses, and telephone numbers of at least three references to: Professor T.P. Ma, Chair, Department of Electrical Engineering, Yale University, 15 Prospect Street, New Haven, CT 06520-2157. Yale University is an affirmative action, equal opportunity employer.

Faculty Position—Departments of Orthopaedic Surgery and Biomedical Engineering. The University of Tennessee-Campbell Clinic Department of Orthopaedic Surgery of the University of Tennessee, Memphis is seeking ■ Ph.D. rehabilitation engineer for an upper level faculty position who will function as Research Director of its Rehabilitation Engineering Program. Candidates shall have demonstrated successful leadership experience in administration, grantsmanship and publications. Academic rank will be commensurate with credentials and experience and will include dual faculty appointments in the Department of Orthopaedic Surgery within the College of Medicine and the Department of Biomedical Engineering within the College of Graduate Health Sciences. Please send Curriculum Vitae or inquiries to: T. David Sisk, M.D., Department of Orthopaedic Surgery, University of Tennessee, Memphis, 800 Madison Avenue, Memphis, Tennessee 38163. The University of Tennessee is an EEO/AA/Title IX/Section 504/ADA employer.

Naval Postgraduate School, Monterey, California, ECE Department invites applications for adjunct and tenure-track positions (all ranks) in the areas of Avionics, Controls, Computers, Communications, Electro-Optics, and Radar/EW Systems. Candidates should possess ■ doctorate in Electrical and/or Computer Engineering, or a closely related field, and be capable of quality instruction and successful research, primarily with MSEE students. The department conducts an advanced level ABET-accredited program awarding MSEE, EE and PhD degrees to military officers of the US and allied nations and DoD employees. Sponsored research opportunities are readily available and extensive computational and laboratory facilities exist. Resumes with publication list, statement of teaching and research interests, via status, and names with addresses of three references should be sent to Dr. Michael A. Morgan, Chairman, Electrical and Computer Engineering Department, Code EC, Naval Postgraduate School, Monterey, CA 93943. Equal Opportunity, Affirmative Action Employer.

The University of Missouri-Columbia Department of Electrical and Computer Engineering invites applications for several tenure-track positions at the assistant level in the areas of computer engineering, computer science, or electrical engineering. Responsibilities include teaching undergraduate and graduate courses, student advising and developing and conducting sponsored research programs. Candidates must have an earned doctorate in Electrical or Computer Engineering, Computer Science or related discipline, and the potential for, and commitment to, developing sponsored research. Candidates for the electrical engineering position must have an interest and background in molecular beam epitaxial growth. Candidates for the computer engineering position should have an interest and background in artificial intelligence, neural networks, fuzzy logic, computer vision or pattern recognition. Interested applicants should send ■ resume, ■ description of research interests, and immigration status for non-United States citizens, as well as ■ description of research interests to: Jon Meese, Chairman, Department of Electrical and Computer Engineering, University of Missouri-Columbia, Columbia, Missouri 65211. The University of Missouri is an Affirmative Action/Equal Opportunity Employer.

Government/Industry Positions Open

Electrical Engineer. Full-time position. Prevailing wage is offered. Laser system & electro-optics development, digital & analog circuit design & computer control design, optical dimensional measurement research. Ph.D. in E.E., 2 yrs. exp. in design & development of laser scanning, computer controlled optical system, digital & analog circuit & microwave engineering & 1 yr. exp. in optical dimensional measurement research, knowledge of ultrafast opto-electronics & waveform sampling req'd. Send resume to Mr. LAU, 7901-C Cessna Ave., Gaithersburg, MD 20879.

Electrical Engineers—Ten (10) Immediate Openings. A unique and highly specialized electrical contractor to the electric power industry is seeking ten (10) experienced Electrical Engineers for its Business Development Department. The successful candidates shall have ■ Bachelors Degree in Electrical Engineering and at least two (2) years experience in the transmission line construction and/or maintenance department(s) of an electric power utility. The positions require excellent verbal and written communication skills, excellent time management skills, the ability to work both cooperatively and independently and the ability to travel within a defined geographic region in the United States. Education, training and/or experience in business development, sales and marketing is desirable. Compensation shall be comprised of ■ base salary/draw commensurate with qualifications, commissions, and bonus incentives. A comprehensive benefits program may be provided upon qualification. Interested candidates should send their resumes to D. Michael Campbell, P.O. Box 2826, Miami, FL 33243.

Wanted: Translators, Japanese to English, Freelance Electrical, Electronic and Computer Engineers (all specialties) needed as freelance translators of advanced Japanese research papers. Ability to write good technical English ■ must. Also needed are persons with similar qualifications capable of technically correcting and rewriting already existing translations. Write to: Scripta Technica, 7961 Eastern Ave, Silver Spring, MD 20910, Telephone: (301) 588-0484.

Test Engineer for NE Ohio Computer peripheral marketing & manufacturing company to analyze & evaluate new computer hardware products utilizing conventional & advanced test equipment; design/implement maintenance algorithms; design/implement test systems (equipment); analyze & enhance fault-tolerant features; recommend design changes; design test programs & procedures: detect, diagnose, & analyze systems errors for logical/physical failure; assist technicians & engineers in application of test programs & procedures in production. 4 yrs. exp. req. in above duties & a B.S. in Electronic or Computer Engineering (must have taken at least 2 courses in electronic devices & circuits (with labs); 2 courses in digital integrated circuits (with labs); 2 courses in electrical & electronics measurement (with labs); & a course in advance systems for measurement & control (with project)). 40 hrs/wk, 8am to 5pm, $41,515/yr. Must have proof of legal authority to work permanently in the U.S. Send resume in duplicate (no calls) to J. Davies, JO 1200885, Ohio Bureau of Employment Service, P.O. Box 1618, Columbus, OH 43216.

Account Manager/Sales Engineer: Using knowledge & understanding of auto electrical architecture & quality; functional performance criteria of electrical & electromechanical products; & applications of new materials via plastics & electronic circuit advancements, provide engineering, quality & commercial negotiation service between customer & division. Interface with customers, resolve quality issues, maintain price files. Maintain knowledge of products including past & present designs & future product areas. Ensure technical specifications of proposed products & program of introduction are in accordance with customers' specifications. Coordinate new product programs with company's engineering operations group to ensure expectations are met on engineering development, delivery of prototypes, product testing & production launching. Coordinate customer product test program, in-process testing & product sign-off. Maintain details of customers' forecasts & plans & obtain information of a commercial, technical & strategic nature relating to customers' competitors. Advise on prod. design, legislative & production matters. Make cost recommendations. Supply info. for vehicle specification records. Submit yearly forecast covering level of business. Train & direct Sales Engineers. Bach. Deg. Elect. Eng. Tech. 2 yrs. on the job exp. to include 2 yrs. exp. working with: low & high current direct switching methods; high side, low side solid state switching; multi-level current &/or voltage protection schemes; custom & non-custom circuit applications; modern day multiplexing schemes; self diagnostic system within sub-

systems; ministry of transportation regulations & applications specific to safety critical items. $48,900/yr, 40+ hr/wk (9:00-5:30). Send resumes to: 7310 Woodward Ave., Rm 415, Detroit, MI 48202, Ref: No. 29992. "Employer Paid Ad."

Field Service Engineer. Monday through Friday; 8:00 a.m. to 5:00 p.m.; 40 hours per week; $42,998.00 annually. Position located in Beaverton, Oregon. Required is a Bachelor of Science Degree in Electrical Engineering Technology and two (2) years of experience in the job being offered or two (2) years of experience as a Commissioning Engineer on thyristor motor control systems. In lieu of a Bachelor's Degree, employer will accept an Associate Degree in Electrical Engineering Technology with two (2) years of experience as a Commissioning Engineer on thyristor motor control systems. As part of the required experience in the position being offered or in the related occupation, the applicant must have trained customers and/or company personnel in the use and maintenance of motor control systems and actively participated in the commissioning of thyristor motor control systems with programmable controller interface. Applicant must be fluent in speaking, reading and writing the Swedish language. Incumbent applies electrical engineering principles in overseeing commissioning, service, and customer support of the company's Swedish-designed rolling mills, paper machine and winders, large thyristor rectifiers, and crane drive systems. Participates in system design with other department engineers based upon Swedish proprietary designs and U.S. customer requirements. Supervises company and customer personnel during system check-out and site start-up. Reviews, analyzes and enhances new designs from Sweden. Develops and implements training programs for company and customer personnel in systems operation, including parameter settings and use of control tools to achieve maximum performance and efficiency from profile rolling mill and related systems. Confers regularly with Swedish design engineers for company operations abroad to resolve complex issues relative to field installation of drive systems. Applies engineering knowledge of software and hardware in developing new interfaces for customized static and dynamic process pictures for man-machine communication. Corrects and assembles system documentation into final format following commissioning of systems. Performs customer service in engineering repairs and initiates systems modification and system additions as required. Extensive communication in Swedish is required. Interested applicants submit resume to: Employment Division, Attn: Job Order - 5550336, 875 Union Street N.E. Room 201, Salem, Oregon 97311. An employer paid ad.

National Manager Engineering Services. Eastern Electric, an industry leader with Engineering Service and remanufacturing locations coast-to-coast, is seeking a hands-on, results-oriented professional to fill this key operations position. This Princeton, NJ based position will report to the CEO and will have responsibility for expanding and overseeing the Nationwide Engineering Service Function. Qualified candidates will possess an Electrical Engineering Degree and a minimum 15 years experience in various management (P&L responsibility) and field positions in the Power Delivery field. Specific experience must include: —Testing, Calibration, Repair & Installation. Substations; Breakers; Relays; AC & DC Drives. —Power System Studies. —Predictive & Preventative Maintenance. An extremely competitive salary, benefits and incentive compensation package with the possibility of stock options. Only qualified individuals should forward a detailed resume and salary history to: Eastern Electric P.O. Box 7588 Princeton, NJ 08543-7588

Consultant in Operations Research & Operations Management to build mathematical-stochastic-programming-based logistics & manufacturing models. Specific responsibilities include obtaining all necessary data from client, performing management & operations analyses to determine model requirements & building models that meet client requirements. Models are calibrated to client needs through frequent interaction & translated into computer software on a number of hardware platforms & tested using client data. Software systems are installed at client site for use in operational decision-making. Requires Ph.D. in Operations Research & 1 yr exp. in Job Offered or 1 yr exp. researching Probabilistic Modelling & Analysis (exper. gained in Ph.D. program acceptable). Candidate must also possess demonstrated expertise in cyclic scheduling of unreliable machines; dem knowledge of combinatorial & dynamic optimization; dem knowl of operations management for manufacturing & distribution applications & dem exp in numerical computation for optimization. Employment location in greater Boston, Massachusetts, area. Salary $57,500/yr; M-F 9-5. Send resumes to: MASS DET, P.O. Box 8968, Boston, MA 02114. Attn: Job Order # 2851. EOE. Applicants must be U.S. workers presently authorized to work in the United States on a full-time, permanent basis.

Government/Industry Position Wanted

Math M.S. 25 yrs R&D, pubs guid waves sys seeks 2-4 mo pos Num Meth-coding Fortran/Rocky Mtn Basic have PC486 (303)494-8405.

Antennas Engineer: Ph.D. (1986). 14 years of research, teaching and industrial experience in antennas and electromagnetic waves. Over 40 publications and 2 patents on reflector antennas. Contact Mohamed at (408) 248-2742.

Des.1-5Ghz 1Kwatt A.M.Tran.25kyr.214-596-8319.

PROFESSIONAL CONSULTING SERVICES

ADVERTISING RATES

1 Insertion—$320 12 Insertions—$3840

50% discount to IEEE members on three or more insertions.
If you are an IEEE member, please enclose your membership number with the order.
Copy cannot exceed 1-inch in depth.
No product may be offered for sale.
Advertising restricted to professional engineering and consulting services.
No orders can be accepted by telephone; order and copy must be sent together.
For any further information and closing dates please contact:
Advertising Production Dept., 212-705-7578.

CONSULTING & PROTOTYPES

ELECTRIC MOTORS

BRUSHLESS MOTORS SWITCHED RELUCTANCE
STEPPING MOTORS AC INDUCTION

MAGNA PHYSICS CORP.
100 Homestad Ave.
P.O. Box 78
HILLSBORO, OH 45133

JAMES R. HENDERSHOT
TEL: 513-393-9835
513-393-3810
FAX: 513-393-9836

THE CONSULTING GROUP

Multi-Disciplined Engineers with P.E./Ph.D.
- Microwave, RF, Fiber-Optic Systems Design
- Oscillators, Amplifiers, Filters, Antennas, Synthesizer/PLL Design. Microprocessor, Communication ckts. Industrial Power System. R&D, Prototyping & Testing in our Lab facilities.

119-40 Metropolitan Ave., Kew Gardens, NY 11415
Ph. (718) 846-5400 Fax (718) 846-2440

International Compliance Corporation

Design, Test, & Consulting
- FCC Certification/Verification
- VDE, CISPR, VCCI (Japan)
- "1992" European Compliance Testing
- Product Safety: UL, CSA, IEC, VDE
- Electrostatic Discharge (ESD)
- MIL-STD 461/462, NARTE-Certified Engineers

1911 E. Jeter Rd (817) 491-3696
Argyle, TX 76226-9401 FAX: (817)-491-3699

INTEGRATED CIRCUIT DESIGN CONSULTING

Providing integrated circuit design and analysis consulting services with gate arrays, cell libraries, or full custom in digital, analog, cmos, bipolar or ecl technologies and support services such as modeling, layout, verification, software, testing, debugging, documentation, and reverse engineering.

1556 Halford Ave, Ste 310 Santa Clara, CA 95051
(408) 243-7422

RAINES ELECTROMAGNETICS

Consulting Since 1972
- Antennas and Arrays
- Scattering and Radar Cross Sections
- Radhaz & Environmental Impact
- Simulations of Fields & Phenomena

Jeremy K. Raines, Ph.D. (MIT), P.E.
13420 Cleveland Drive (301) 279-2972
Potomac, Maryland 20850-3603

IOCC

INTEGRATED OPTICAL CIRCUIT CONSULTANTS

Consulting, Contract R&D, and Prototyping
Integrated, Fiber, and Guided-Wave Optics
- Applications Engineering
- Design, Fabrication and Evaluation
- Critical Analysis of Technology
- Troubleshooting
- Marketing

R.A. Becker, D. Sc.
President
(408) 446-9812

10482 Chisholm Ave.
Cupertino, CA 95014

O.E.M. Electronic Products
- *13 Year Product Development History*
- *Custom, RF/Digital ASICs • RF Systems*
- *Computerized Instrumentation*
- *Spread Spectrum Communications*
- *Hitachi Authorized Design Center*

LocUS, Incorporated

1842 Hoffman St., Madison, WI 53704
608/244-0500 FAX 608/244-0528

CONTROL SYSTEM CONSULTING
- Servo design, high performance motion control, synthesis, system performance, simulation, specs, integration, testing
- Electrical, mechanical, hydraulic
- Defense, aerospace, industrial experience

30 East Gate Road A.R. Hazelton
Danbury, Conn. 06811 (203) 743-7002

T-TECHTM 1 DEAN ST./BOX 151
HUDSON, MASS.
VOICE: (508) 562 5820 FAX: (508) 568 1219

RF (TO 2 GHz), ANALOG, VIDEO,
FIBER OPTICS, PLL'S, SYNTHESIZERS,
FILTERS, A/D CONVERSION

THE MOST TIMELY, COST EFFECTIVE,
AND HIGHEST PERFORMANCE SOLUTION.

Princeton Electro-Technology, Inc.

PERMANENT MAGNETS

MATERIALS, DEVICES & APPLICATIONS

CONSULTING, DESIGN, PROTOTYPES, MARKETING

Peter Campbell, Ph.D., President
2449 Patricia Avenue **Tel: (310) 287-0375**
Los Angeles, CA 90064 **Fax: (310) 287-0378**

IRA J. PITEL, Ph.D.

Consulting, Research and Development in Power Electronics and Magnetics

Power Supplies, Inverters, Converters, Motor Drives, Lighting Controls, Industrial Controls, Transformers, and Special Magnetics.

MAGNA-POWER ELECTRONICS, INC.
135 Route 10 Whippany, NJ 07981
(201) 428-1197

Patent Attorney

Robert E. Malm, Ph.D. (M.I.T.)
Attorney At Law
Post Office Box 522
Pacific Palisades, CA 90272
Tel: (310) 459-8728
Fax: (310) 573-1781

INDUSTRIAL CONTROLS

CUSTOM MICROPROCESSOR CONTROLS
- Machine Tool Controls
- Process Controls
- Medical Electronics
- Neural Networks
- Consumer Product Design
- Instrument Design
- Prototype Production
- Control Software

Wintriss Engineering Corporation
4715 Viewridge, San Diego 92123
(800) 733-8089 Vic Wintriss, MSEE

NOISE, TRANSIENTS AND INTERFERENCE
- FCC, VDE, EMC/EMI
- Susceptibility, ESD, RF, Transients, Lightning
- Testing & Retrofit for Product Enhancement
- Speed to Market via Design Review
- Noise-Immune Designs and Prototypes
- FCC Compliance Training & Retrofits

TKC THE KEENAN CORPORATION
(813) 544-2594

R. Kenneth Keenan, Ph.D.
Vice President, Engr.
8609 66th St. North
Pinellas Park, FL 34666

SOFTWARE ENGINEERING
- Real-Time Systems Analysis and Design
- Software Engineering Training (Call for Offerings)
- CASE Training and Implementation
- Consulting Services
- Product Development

Carl A. Argila, Ph.D., Inc.
SOFTWARE ENGINEERING CONSULTANT
800-347-6903

ELECTRONIC AND SOFTWARE DESIGN

Top Notch Engineering Firm is experienced in:
- Electro-Chemistry
- Electro-Mechanical
- System Design & Analysis
- Customized Test Equipment
- Electro-Optics
- Software Development
- Feasibility Studies
- Fast Turn Prototypes

ELITE ENGINEERING CORP. (805) 494-1033
741 Lakefield Road, Suite C, Westlake Village, CA 91361

LEONARD R. KAHN, P.E.

Consultant in Communications and Electronics
Single Sideband and Frequency Shift Systems
Diversify Reception - Stereophonic Systems
Modulation Systems
Registered Patent Agent

222 Westbury Ave.
Carle Place, NY 11514
516-222-2221

ELECTROMAGNETIC DESIGN ANALYSIS

Consultancy by world leaders in 3D electromagnetic computation using PE2D, OPERA, TOSCA and ELEKTRA
- electrical machines
- recording heads
- actuators
- transformers
- loudspeakers
- MRI scanners
- magnetic casting
- scientific apparatus
- NDT equipment
- accelerator magnets

VECTOR FIELDS INC. tel: (708) 851-1734
1700 N Farnsworth Ave, Aurora IL 60505 fax: (708) 851-2106

PERFORMANCE ENGINEERING

CONTROL SYSTEM PROTOTYPES
SPECIALTY MANUFACTURING
STABILIZATION SYSTEMS
PERFORMANCE TUNING
MILITARY/INDUSTRIAL

DIGITAL DESIGNS
O.O.D. SOFTWARE (Ada)
SIMULATIONS
PERFORMANCE UPGRADES
LOW COST SOLUTIONS

Jack Hebert
MGR TECH MKTG

TEL 413-663-8010
FAX 413-663-6820

Editorial Offices: New York City 212-705-7555 San Francisco 415-282-3608 Washington, DC 202-544-3790

EDITORIAL CORRESPONDENCE. IEEE Spectrum, 345 East 47th St., New York, N.Y. 10017, Attn: Editorial Dept. Responsibility for the substance of articles published rests upon the authors, not the IEEE or its members. Letters to the editor may be excerpted for publication.

REPRINT PERMISSION. Libraries: Articles may be photocopied for private use of patrons. A per-copy fee (indicated after the code appearing at the bottom of the first page of each article) must be paid to the Copyright Clearance Center, 29 Congress St., Salem, Mass. 01970. *Instructors:* Isolated articles may be photocopied for noncommercial classroom use without fee. *Other copying or republication:* Contact: Editor, *IEEE Spectrum*.

ADVERTISING CORRESPONDENCE. IEEE Spectrum, 345 East 47th St., New York, N.Y. 10017, Attn: Advertising Dept., 212-705-7760. Also see Advertising Sales Offices listing on last page. The publisher reserves the right to reject any advertising.

COPYRIGHTS AND TRADEMARKS. IEEE Spectrum is a registered trademark owned by The Institute of Electrical and Electronics Engineers, Inc. EEs' tools & toys, Faults & failures, Innovations, Legal aspects, Managing technology, Newslog, Program notes, Reflections, Speakout, Spectral lines, Spinoffs, Technically speaking, The engineer at large, and Whatever happened to? are trademarks of the IEEE.

GENERAL INQUIRIES: 1-800-678-IEEE; Headquarters: 345 East 47th St., New York, N.Y. 10017, 212-705-7900. *Tel. extensions at headquarters:* General Manager, 7910; Public Relations, 7369; Publishing Services, 7560. *At other locations:* Regional Activities, Section Services, Educational Activities, 908-981-0060, or write to IEEE Service Center, Box 1331, Piscataway, N.J. 08855; Membership Services, 908-981-0060; Professional Services, 202-785-0017; Technical Activities, 908-562-3900.

Scanning
The Institute

Powers named IEEE general manager

John H. Powers was named general manager of the IEEE, effective July 13, 1992. He joined the IEEE in December 1990 as associate general manager for volunteer services.

Powers succeeded Eric Herz, who will retire Dec. 31. For the remainder of the year, Herz will continue as executive director of the IEEE, a title he has held along with that of general manager since 1979. Herz will work closely with Powers "to ensure a smooth, efficient transition in the overall management of our worldwide operations and activities," said IEEE President Merrill W. Buckley Jr.

"As the IEEE's senior staff executive for the past 14 years, Eric Herz has contributed significantly to our noteworthy growth over this period," Buckley noted. "During his tenure, the Institute emerged as the world's largest technical professional organization." He pointed out that since Herz became general manager, the IEEE had grown from 190 000 members to more than 320 000 members in 145 countries. Also during Herz's stewardship, annual revenues more than quadrupled to US $115 million. The IEEE currently employs some 500 people primarily in New York City, Piscataway, N.J., and Washington, D.C.

Before joining the IEEE staff, Powers had been with IBM Corp. for 26 years, advancing through a number of senior management positions. Just before coming to the IEEE, he was manager of manufacturing technical and business operations in IBM's East Fishkill, N.Y., facility. Powers' appointment as general manager concluded an eight-month search involving more than 400 applicants.

Powers was also named an IEEE Fellow in 1990 "for contributions to and leadership in manufacturing technology." He is a past president of the IEEE Components, Hybrids and Manufacturing Technology Society and served as chairman of the joint committee on semiconductor manufacturing. He was also chairman of the editorial board of the IEEE Transactions on Semiconductor Manufacturing. Powers holds a bachelor of science degree in electrical engineering from Stevens Institute of Technology and a master of science degree from Union College.

Court brief favors reverse engineering

IEEE-United States Activities joined an *amicus curiae* brief supporting the right of small entrepreneurs to manufacture and distribute software products developed through reverse engineering. The friend-of-the-court brief, filed in San Francisco by the American Committee for Interoperable Systems of Washington, D.C., asked a U.S. court of appeals to overturn a lower court ruling that outlawed the practice.

In *Sega v. Accolade*, a U.S. district court held that any reproduction of a software work, down to the printing of a single page of decompiled computer code, infringes on a copyright.

"The disassembly of computer code for study, whether or not commercially motivated, is necessary for technological progress in software engineering," said Arvid G. Larson, an IEEE Vice President and head of IEEE-USA. "We do not believe the courts should use sanctions of the copyright law to help computer equipment manufacturers lock 'unauthorized' software out of the equipment they sell to the public."

Larson said that prohibiting reverse engineering would stifle innovation and competition, and would be disastrous to the fast-growing computer software industry in the United States.

Coming
in Spectrum

SUPERCOMPUTING. This high-tech endeavor is one of the few in which the United States still clings to a lead in many areas. It also is vital to future breakthroughs in science and engineering. This special report will analyze the field from half a dozen viewpoints.

- Parallelism. Companies the size of IBM Corp. and Digital Equipment Corp., as well as the more focused firms, like Thinking Machines, Intel, and Ncube, are making remarkable progress with massively parallel architectures.
- Hardware. The leading edge in emitter-coupled logic and gallium arsenide is married to advanced cooling and packaging techniques.
- Networks. The status of National Science Foundation networks, as well as local high-performance types like CERFnet and the Gore proposal, are reviewed.
- Software. Massively parallel operating systems, languages, and compilers. . .you name it, it's needed.
- Applications. Expected to reach rates of a trillion floating-point operations per second in just five years, supercomputers will take on challenging, unprecedented assignments, especially in engineering.
- Japan. Frenetic activities and impressive successes characterize Japanese experimental and commercial supercomputing.
- Visualization. This technology has a ways to go before it can live up to its early billing —but the payoffs could be tremendous.

"The importance of the program cannot be overlooked ... it so fundamentally alters the mechanics of mathematics."
New York Times

"Mathematica is a startlingly good tool."
Nature

"Mathematica has the potential to change the world of science at least as much as word processing has changed the world of writing."
InfoWorld

Mathematica®

A System for Doing Mathematics by Computer

Function: Numerical, symbolic, graphical computation, interactive programming. Integrated technical computing environment.

Numerical Computation: Arbitrary-precision arithmetic, complex numbers, special functions (hypergeometric, elliptic, etc.), combinatorial and integer functions. Matrix operations, root finding, function fitting, Fourier transforms, numerical integration, numerical solution of differential equations, function minimization, linear programming.

```
In[1]:=
 3^70
Out[1]=
 2503155504993241601315571986085849
In[2]:=
 Hypergeometric2F1[7,5,4.1,3-I]
Out[2]=
 -0.00403761 - 0.00295663 I
```

Numerical Computation

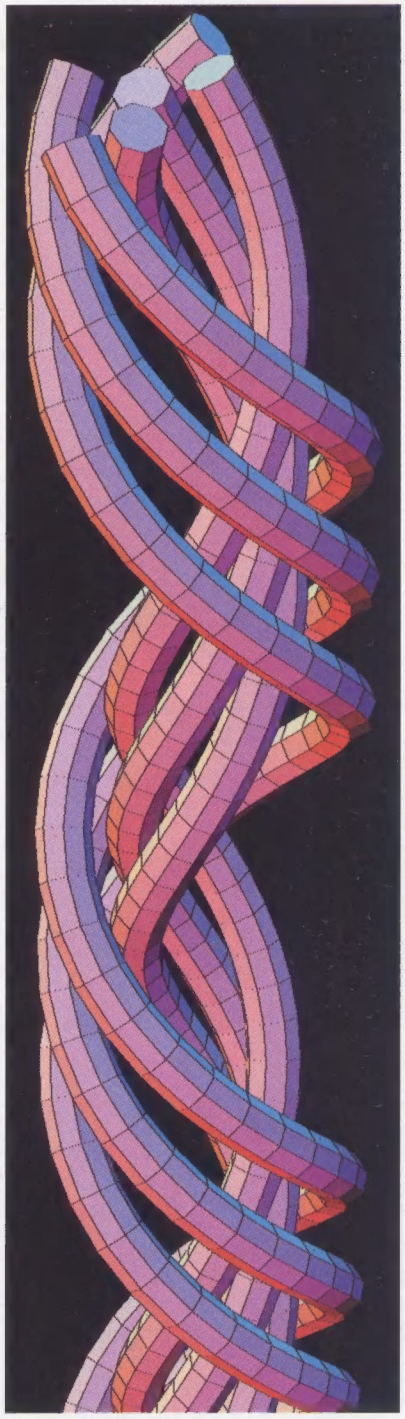
Symbolic Computation: Equation solving, symbolic integration, differentiation, power series, limits. Algebraic operations, polynomial expansion, factorization, simplification. Operations on matrices, tensors, lists, strings.

Graphics and Sound: 2D, 3D plots of functions, data, geometrical objects. Contour, density plots. 3D rendering with intersecting surfaces, lighting models, symbolic descriptions. Combining and labeling graphics. Color PostScript output, publication quality graphics, animation (most versions). Sampled sound generation from functions and lists.

```
In[1]:=
 Integrate[x/(a + Exp[x]), x]
Out[1]=
                                  x Log[1 + E^x/a]
 x^2/(2a) - ------------------ -
                    a
                                  PolyLog[2, -(E^x/a)]
            ---------------------
                    a
```

Symbolic Computation

Programming: High-level, interactive, symbolic system. Full procedural language, functional programming constructs. General transformation rule paradigm based on pattern matching.



Graphics and Visualization

External Interface: Input from external files, programs. Expressions, strings, words, records, numbers (in *Mathematica* or Fortran format), with arbitrary word and record delimiters. Output in TeX, C, Fortran, PostScript. System functions, file manipulation. External function calls, general interprocess communication, and data exchange via *MathLink*™.

Notebook Front End (Macintosh, NeXT, Microsoft Windows): Based on word processor analogy. Notebook interactive documents mixing text, graphics, animations, *Mathematica* input, output. On NeXT and Macintosh, front ends can be used with kernels on other computers, and support sound.

Documentation: *Mathematica: A System for Doing Mathematics by Computer*, Second Edition, by Stephen Wolfram (Addison-Wesley, 1991) available at bookstores. Additional documentation supplied with specific versions. *The Mathematica Journal* published quarterly by Miller Freeman. Many other *Mathematica* books also now available.

Versions Available: Macintosh • MS-DOS • Microsoft Windows • CONVEX • DG AViiON • Digital Equipment Corporation VAX/VMS, RISC ULTRIX • HP 9000 • HP Apollo • IBM RISC Systems/6000 • MIPS • NeXT • Silicon Graphics • Sony • Sun -3 and SPARCstations • Educational, volume, reseller, and other discounts available • Now shipping Version 2.

```
log[1] = 0
log[E] = 1
log[x_ y_] := log[x] + log[y]
log[x_^n_] := n log[x]
log'[x_]:= 1/x     (* derivative *)
log/: InverseFunction[log] = exp
log/:
Series[log[x_], {x_, 1, n_}] :=
 Sum[-(-1)^k (x-1)^k/k, {k,1,n}] +
                      0[x,1]^(n+1)
```

High-Level Programming

Implementation: 843 pre-defined *Mathematica* functions (kernel C source 330,000 lines).

Typical Applications: Research, engineering, education, mathematical modeling, publication graphics, data analysis, visualization, systems analysis, algorithm development.

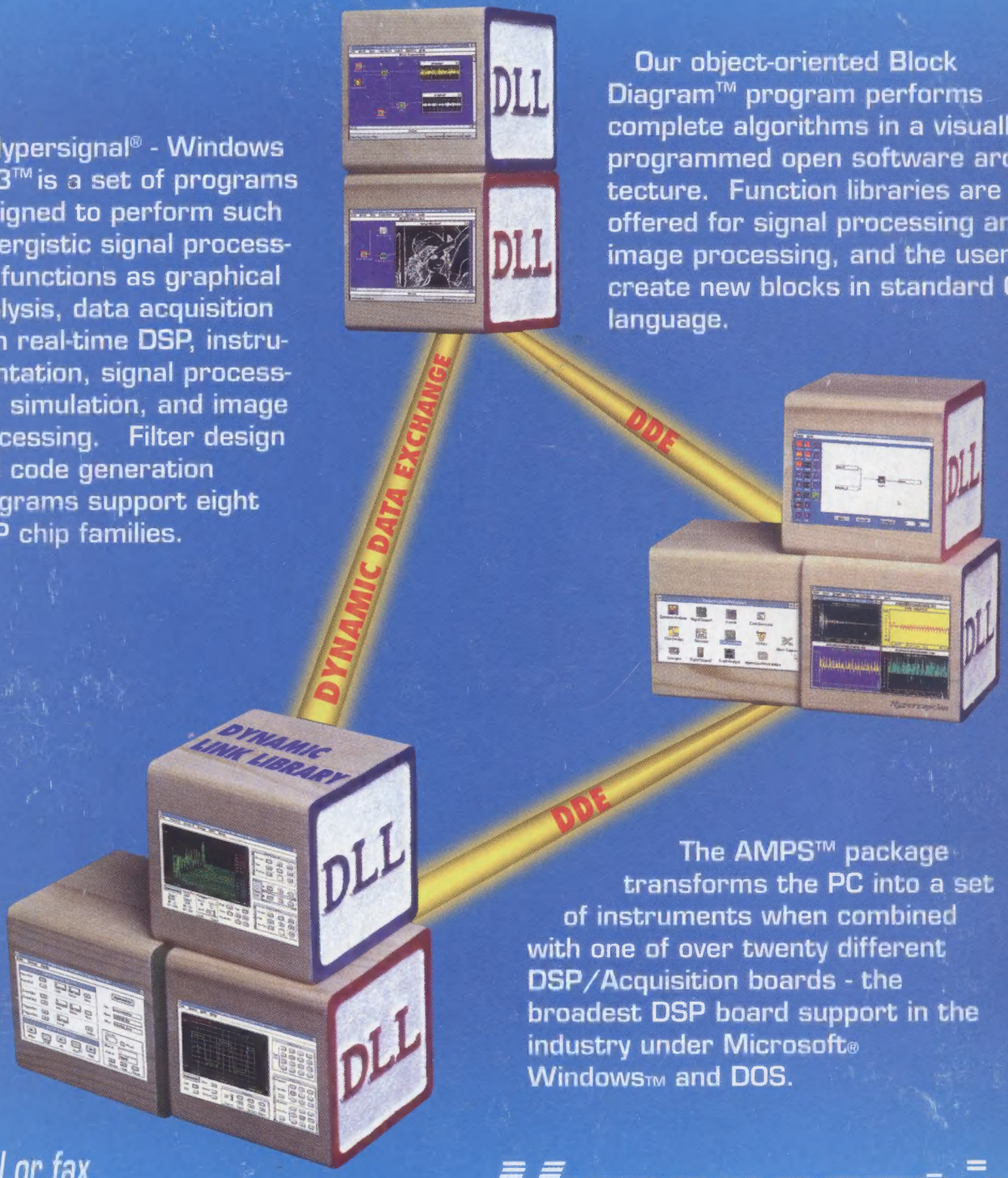
Awards: *MacWelt*, 1991 • *Macworld*, 1990-91 • *Discover*, 1990 • *BYTE*, 1989 • *MacUser*, 1989 • *Business Week*, 1988 • *InfoWorld*, 1988

Wolfram Research, Inc.
100 Trade Center Drive, Champaign, IL 61820-7237, USA.
Information: 217-398-0700. Orders: 800-441-MATH.
Email: info@wri.com. Or visit your local software dealer.

Circle No. 17

Finally...
A Comprehensive Digital Signal Processing Environment

Hypersignal® - Windows RT-3™ is a set of programs designed to perform such synergistic signal processing functions as graphical analysis, data acquisition with real-time DSP, instrumentation, signal processing, simulation, and image processing. Filter design and code generation programs support eight DSP chip families.



Our object-oriented Block Diagram™ program performs complete algorithms in a visually programmed open software architecture. Function libraries are offered for signal processing and image processing, and the user can create new blocks in standard C language.

The AMPS™ package transforms the PC into a set of instruments when combined with one of over twenty different DSP/Acquisition boards - the broadest DSP board support in the industry under Microsoft® Windows™ and DOS.

Call or fax for more information:

ph: (214) 343-8525 fax: (214) 343-2457
9550 Skillman LB 125 • Dallas, Texas 75243

Hyperception

The Leader In DSP

International Distributors:

AUSTRALIA - Electro Optics PTY, LTD.: phone +61-2-654-1873; FAX +61-2-654-1539. DENMARK - Assentoft Electronics: phone +45-86-16-29-26; FAX +45-86-16-20-12. FINLAND - ITT: phone +358-90-739100; FAX +358-90-701-5683. FRANCE - Logabex: phone +33-61-80-94-37; FAX +33-61-20-95-49. ISRAEL - IES,LTD,: phone +972-3-7526333; FAX +972-3-7510927. KOREA - Seoil Enterprise Co.: phone +82-2-237-0872; FAX +82-2-237-0874. SINGAPORE - Bliss Services PTE LTD.: phone +65-3381300; FAX +65-3381900. TAIWAN, ROC - Exartech International Corporation: phone +886-2-977-6828; FAX +886-2-977-6829.

Circle No. 13